RACOM
RADIO DATA NETWORKS

Operating manual

M!DGE
– GPRS/UMTS/HSPA+/LTE router

1.8
12/7/2015

RACOM s.r.o. • Mirova 1283 • 592 31 Nove Mesto na Morave • Czech Republic
Tel.: +420 565 659 511 • Fax: +420 565 659 512 • E-mail: racom@racom.eu

www.racom.eu

Table of Contents

Important Notice 5
Getting started 6
1. M!DGE router 7
    1.1. Introduction 7
    1.2. Key features 7
    1.3. Standards 8
2. M!DGE in detail 9
3. Implementation notes 11
    3.1. Ethernet SCADA protocols 11
    3.2. Serial SCADA protocols 11
    3.3. Network center 11
    3.4. VPN tunnels 11
4. Product 12
    4.1. Dimensions 12
    4.2. Connectors 12
    4.3. Indication LEDs 16
    4.4. Technical specifications 17
    4.5. Model offerings 18
    4.6. Accessories 18
5. Bench test / Step-by-Step guide 20
    5.1. Connecting the hardware 20
    5.2. Powering up your wireless router 20
    5.3. Connecting M!DGE to a programming PC 20
    5.4. Basic setup 21
6. Installation 22
    6.1. Mounting 22
    6.2. Antenna mounting 22
    6.3. Grounding 22
    6.4. Power supply 22
7. Web Configuration 23
    7.1. HOME 23
    7.2. INTERFACES 24
    7.3. ROUTING 54
    7.4. FIREWALL 61
    7.5. VPN 67
    7.6. SERVICES 78
    7.7. SYSTEM 101
    7.8. LOGOUT 121
8. Command Line Interface 122
    8.1. General usage 122
    8.2. Print help 123
    8.3. Getting config parameters 124
    8.4. Setting config parameters 124
    8.5. Updating system facilities 125
    8.6. Manage keys and certificates 125
    8.7. Getting status information 126
    8.8. Scan 127
    8.9. Sending e-mail or SMS 127
    8.10. Restarting services 127
    8.11. Debug 128
    8.12. Resetting system 129

8.13. Rebooting system 129
8.14. Running shell commands 129
8.15. CLI commands history 129
8.16. CLI–PHP 130
9. Troubleshooting 135
9.1. Common errors 135
9.2. Messages 135
9.3. Troubleshooting tools 135
10. Safety, environment, licensing 137
10.1. Safety instructions 137
10.2. Country of Origin 139
10.3. Warranty 140
A. Glossary 141
Index 143
B. Revision History 145

List of Figures

1. Router M!DGE UMTS and M!DGE LTE 6
2.1. M!DGE front and terminal panel 9
4.1. Dimensions in millimeters 12
4.2. Antenna connectors SMA 12
4.3. 2× Eth RJ45 Plug - pin numbering 13
4.4. USB connector 13
4.5. Screw terminal 14
4.6. Reset button 15
4.7. Indication LEDs 16
4.8. Flat bracket 18
4.9. Demo case 19
6.1. Grounding 22
10.1. Country of Origin declaration 139

List of Tables

4.1. Pin assignment Ethernet interface 13
4.2. USB pin description 13
4.3. Screw terminal pin assignment 14
4.4. Digital input levels 14
4.5. Digital output parameters 14
4.6. Voltage Polarity connector misconnection Risks 15
4.7. M!DGE interfaces and status indicators 16
4.8. Technical specifications 17

Important Notice

Copyright

© 2014 RACOM. All rights reserved.
Products offered may contain software proprietary to RACOM s. r. o. (further referred to under the abbreviated name RACOM). The offer of supply of these products and services does not include or inply any transfer of ownership. No part of the documentation or information supplied may be divulged to any third party without the express written consent of RACOM.

Disclaimer

Although every precaution has been taken in preparing this information, RACOM assumes no liability for errors and omissions, or any damages resulting from the use of this information. This document or the equipment may be modified without notice, in the interests of improving the product.

Trademark

All trademarks and product names are the property of their respective owners.

Important Notice

- Due to the nature of wireless communications, transmission and reception of data can never be guaranteed. Data may be delayed, corrupted (i.e. have errors), or be totally lost. Significant delays or losses of data are rare when wireless devices such as the M!DGE/MG102i are used in an appropriate manner within a well-constructed network. M!DGE/MG102i should not be used in situations where failure to transmit or receive data could result in damage of any kind to the user or any other party, including but not limited to personal injury, death, or loss of property. RACOM accepts no liability for damages of any kind resulting from delays or errors in data transmitted or received using M!DGE/MG102i, or for the failure of M!DGE/MG102i to transmit or receive such data.
- Under no circumstances is RACOM or any other company or person responsible for incidental, accidental or related damage arising as a result of the use of this product. RACOM does not provide the user with any form of guarantee containing assurance of the suitability and fit for purpose.
- RACOM products are not developed, designed or tested for use in applications which may directly affect health and/or life functions of humans or animals, nor to be a component of similarly important systems, and RACOM does not provide any guarantee when company products are used in such applications.

Getting started

M!DGE Wireless Routers will only operate reliably over the cellular network if there is a strong signal. For many applications a flexible stub antenna would be suitable but in some circumstances it may be necessary to use a remote antenna with an extension cable to allow the antenna itself to be positioned so as to provide the best possible signal reception. RACOM can supply a range of suitable antennas.

1. **Install the SIM card**
   Insert a SIM card into the SIM socket. Make sure the SIM is enabled for data transmission.
2. **Connect the GSM/UMTS antenna**
   Fit a GSM/UMTS antenna. If needed, contact RACOM for suitable antennas and other details.
3. **Connect the LAN cable**
   Connect one M!DGE Ethernet port to your computer using an Ethernet cat.5 cable
4. **Connect the power supply**
   Connect the power supply wires to the M!DGE screw terminals, ensuring correct polarity. Switch on the power supply.
5. **Setting of IP address of the connected computer**
   By default the DHCP server is enabled, thus you can allow the Dynamic Host Configuration Protocol (DHCP) on your computer to lease an IP address from the M!DGE. Wait approximately 20 seconds until your computer has received the parameters (IP address, subnet mask, default gateway, DNS server).
   As an alternative you can configure a static IP address on your PC (e.g. 192.168.1.2/24) so that it is operating in the same subnet as the M!DGE. The M!DGE default IP address for the first Ethernet interface is 192.168.1.1, the subnet mask is 255.255.255.0.
6. **Start setting up using a web browser**
   Open a web browser such as Internet Explorer or Firefox. In the address field of the web browser, enter default IP address of M!DGE (i.e. http://192.168.1.1); initial screen will appear. Follow the instructions and use the M!DGE Web Manager to configure the device. For more details see Chapter 7, *Web Configuration*.

Fig. 1: Router M!DGE UMTS and M!DGE LTE

Note

M!DGE can be safely turned off by unplugging the power supply.

1. M!DGE router

1.1. Introduction

Although M!DGE wireless routers have been specifically designed for SCADA and telemetry, they are well suited to a variety of wireless applications. M!DGE HW and SW are ready to maintain reliable and secure connections from a virtually unlimited number of remote locations to a central server. Both standard Ethernet/IP and serial interfaces are available. Moreover, two digital inputs and two digital outputs can be used for direct monitoring and control of application devices.

M!DGE versatility is further enhanced by two independent Ethernet ports. These can be configured to either support two independent LANs (e.g. LAN and WAN settings), or simply connect two devices within one LAN (effectively replacing an Eth switch). M!DGE software is based on proven components, including an Embedded Linux operating system and standard TCP/IP communication protocols.

Combining M!DGE with a MG102i two-SIM router in one network is quite straightforward because of fully compatible interface settings and behaviour on all HW interfaces. Thanks to the compact size and versatility of M!DGE, wireless routers prove indispensable in many SCADA and telemetry, as well as POS, ATM, lottery and security/surveillance applications.

M!DGE together with RACOM RipEX radio router offers an unrivalled solution for combining GPRS and UHF/VHF licensed radio in a single network. Even a single RipEX in the center of a M!DGE network allows for efficient use of addressed serial SCADA protocols.

1.2. Key features

Mobile Interface Parameters

- Mobile Connection options: HSPA+, HSDPA, HSUPA, UMTS, EDGE, GPRS, GSM and LTE
- Global connectivity
- Transparent hand-over between 2G and 3G (M!DGE UMTS) or 2G, 3G and 4G (M!DGE LTE)

Power supply

- Redundant dual power input pins
- Input voltage: 10.2 – 57.6 VDC
- Max. power consumption: 5 W

Services /Networking

- Fallback Management
- Connection supervision, Automatic connection recovery
- Quality of Service (QoS)
- OpenVPN, IPsec, PPTP, GRE, Dial-In
- VRRP
- DHCP server, DNS proxy server, DNS update agent
- Telnet server, SSH server, Web server
- NTP
- Device server, Protocol server, SDK
- Port Forwarding (NAPT)
- Firewall, Access Control Lists

Interfaces

- 2 Ethernet ports: LAN, WAN/LAN
- RS232
- 2× DI, 2× DO
- USB host

Diagnostic and Management

- Web interface, CLI available
- File configuration
- OTA SW update
- Advanced troubleshooting
- SMS remote control, SMS and E-mail notification
- SNMPv1/v2c/3

1.3. Standards

EMC	EN 301 489-1 V1.9.2
	EN 301 489-7 V1.3.1
	EN 301 489-17 V2.2.1
	EN 301 489-24 V1.5.1
	EN 300 328 V1.8.1
	EN 300 440-2 V1.4.1
	EN 50 121-3-2:2006
	EN 50 121-4:2006
	EN 55022:2010
	EN 55024:2010
	EN 61 000-6-2:2005
Radio	EN 301511 V9.0.2
	EN 301893 V1.7.1
Electrical Safety	EN 60950-1 +A11:2006/2009 +A1 +A12:2010/2011
	EN 62311:2008
IP rating	IP40
ETH	IEEE 802.3i
	IEEE 802.3u
	IEEE 802.3af

2. M!DGE in detail

Fig. 2.1: M!DGE front and terminal panel

All M!DGE Wireless Routers run M!DGE Software. Software offering the following key features:

- Interfaces and Connection Management (Section 7.2, “INTERFACES”)
  - Dial-out (permanent, on switchover, distributed)
  - Link Supervision
  - Fallback to backup profile
  - SIM and PIN management
  - Automatic or manual network selection
  - Ethernet (LAN, WAN, bridging, IP passthrough, VLAN management)
  - USB (autorun, device server)
  - Serial port (login console, device server, protocol server, SDK)
  - Digital I/O
- Routing (Section 7.3, “ROUTING”)
  - Static Routing
  - Extended Routing
  - Multipath Routes
  - Bridging
  - Mobile IP
  - Quality of Service (QoS)
- Security / Firewall (Section 7.4, “FIREWALL”)
  - NAPT / Port Forwarding
  - Stateful Inspection Firewall
  - Firewall
- Virtual Private Networking (VPN) (Section 7.5, “VPN”)
  - OpenVPN Server/Client
  - IPsec Peer
  - PPTP Server/Client
  - GRE Peer
  - Dial-in Server

- Services (Section 7.6, “SERVICES”)
  - SDK
  - NTP Server
  - DHCP Server
  - DNS Server
  - Dynamic DNS Client
  - E-mail Client
  - Notification via E-mail and SMS
  - SMS Client
  - SSH/Telnet Server
  - SNMP Agent
  - Web Server
  - Redundancy
- System Administration (Section 7.7, “SYSTEM”)
  - Configuration via Web Manager
  - Configuration via Command Line Interface (CLI) accessible via Secure Shell (SSH) and telnet
  - Batch configuration with text files
  - User administration
  - Troubleshooting tools
  - Over the air software update
  - Licensing (extra features)
  - Keys and certificates (HTTPS, SSH, OpenVPN, ...)
  - Legal Notice

3. Implementation notes

3.1. Ethernet SCADA protocols

SCADA equipment with an Ethernet protocol behaves as standard Ethernet equipment from a communications perspective. Thus the communication goes transparently through the GPRS/UMTS/LTE network. The implementation requires heightened caution to IP addressing and routing. NAPT functionality should be used frequently.

3.2. Serial SCADA protocols

A SCADA serial protocol typically uses simple 8 or 16 bit addressing. The mobile network address scheme is an IP network, where range is defined by the service provider (sometimes including individual addresses, even in the case of a private APN). Consequently, a mechanism of translation between SCADA and the IP addresses is required. To make matters worse, IP addresses may be assigned to GPRS (EDGE, UMTS, etc.) devices dynamically upon each connection.

Please read Chapter 1 in the application note "SCADA serial protocols over GPRS routers"[1] which describes how to efficiently solve this problem using RACOM routers.

3.3. Network center

In every network, the center plays a key role and has to be designed according to customer's requirements. Several possible solutions are described in the application note's Chapter 2 – M!DGE / MG102i CENTER[2].

3.4. VPN tunnels

Customer data security arriving through the mobile network is often very important. Private APN is the basic security requirement, but not safe enough for such applications.

VPN tunnels solution is closely connected with the center and is also briefly described in the given application note.

[1] http://www.racom.eu/eng/products/m/midge/app/scada.html
[2] http://www.racom.eu/eng/products/m/midge/app/midge-mg102i_centre.html

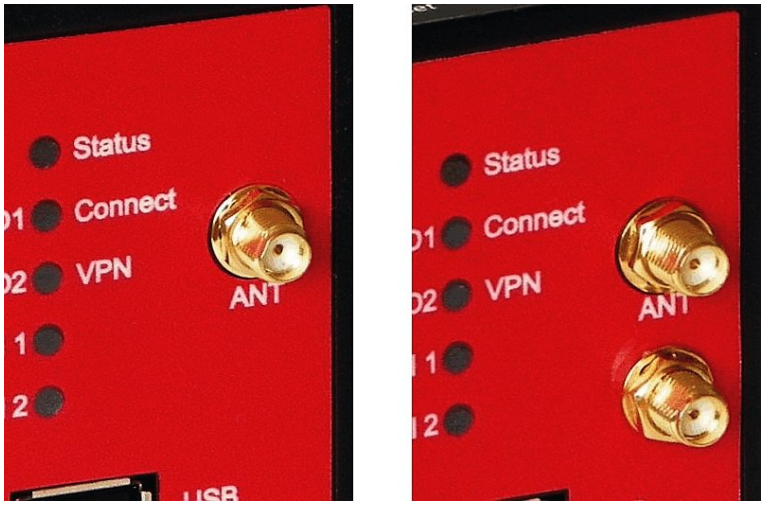
4. Product

4.1. Dimensions

Fig. 4.1: Dimensions in millimeters

4.2. Connectors

4.2.1. Antenna SMA



The UMTS model has one SMA antenna connector.

The LTE model is equipped with two antenna connectors. The ANT connector (above) serves as a main antenna connection, the second connector is auxiliary and serves for better communication with BTS (diversity).

Fig. 4.2: Antenna connectors SMA

4.2.2. 2× Eth RJ45

Tab. 4.1: Pin assignment Ethernet interface

RJ-45 Socket	ETH (Ethernet 10BaseT and 100BaseT)
pin	signal
1	TX+
2	TX−
3	RX+
6	RX−

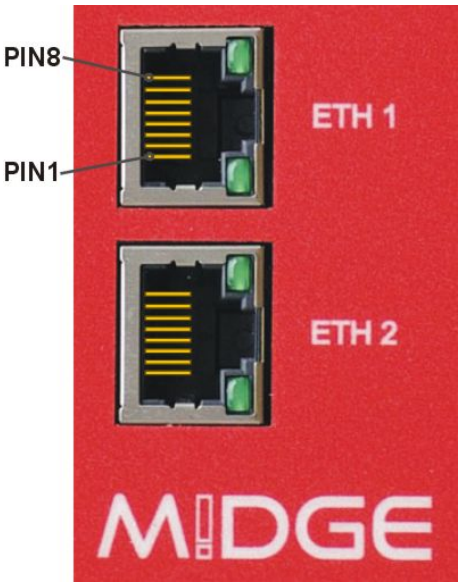


Fig. 4.3: 2× Eth RJ45 Plug - pin numbering

4.2.3. USB

M!DGE uses USB 1.1, Host A interface. USB interface is wired as standard:

Tab. 4.2: USB pin description

USB pin	signal	wire
1	+5 V	red
2	Data (−)	white
3	Data (+)	green
4	GND	black

Fig. 4.4: USB connector

4.2.4. Screw terminal

Screw terminal plug type Stelvio Kontek CPF5/15 or MRT3P/15V01 can be used.

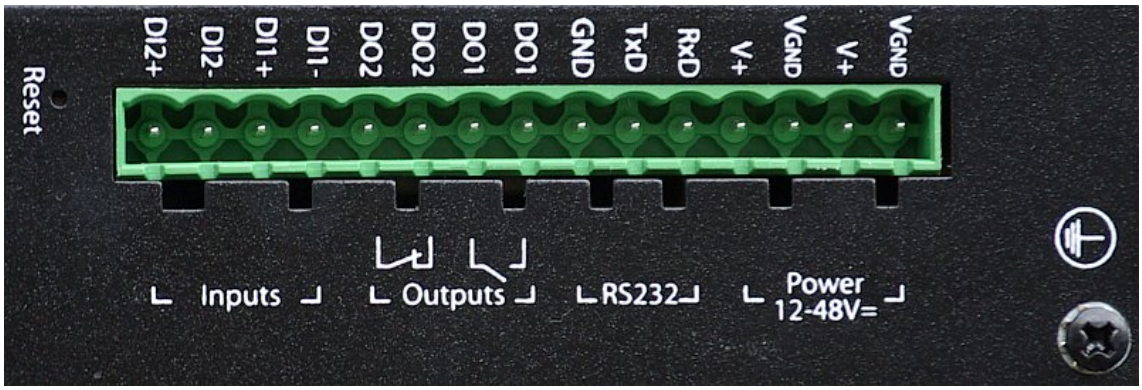


Fig. 4.5: Screw terminal

Tab. 4.3: Screw terminal pin assignment

pin	pin description	signal
1	V_{GND}	Ground internally connected with casing ground.
2	V+ (12–48 V=)	Dual power input - not connected with pin 4: 12–48 VDC (−15 % +20 %) = 10.2–57.6 VDC.
3	V_{GND}	Ground internally connected with casing ground.
4	V+ (12–48 V=)	Dual power input – not connected with pin 2: 12–48 VDC (−15 % +20 %) = 10.2–57.6 VDC.
5	RxD	RS232 – RxD (receiving data)
6	TxD	RS232 – TxD (transmitting data)
7	GND	RS232 – GND (ground)
8	DO1:	Digital output. Dry contact relay. Normally open with M!DGE without powering.
9		
10	DO2:	Digital output. Dry contact relay. Normally open with M!DGE without powering. See Section 7.2.6, “Digital I/O” for details.
11		
12	DI1−	Digital input 1
13	DI1+	Digital input 1
14	DI2−	Digital input 2
15	DI2+	Digital input 2 – see Section 7.2.6, “Digital I/O”

Tab. 4.4: Digital input levels

logical level 0	0 to 5.0 VDC
logical level 1	7.2 to 40 VDC
Note: Negative input voltage is not recognised.	

Tab. 4.5: Digital output parameters

Maximal continuous current	1 A
Maximal switching voltage	60 VDC, 42 VAC (Vrms)
Maximal switching capacity	60 W

Tab. 4.6: Voltage Polarity connector misconnection Risks

pin	pin description		Plug pos.		Plug pos.		Plug pos.		Plug pos.
1	V_{GND}	–	**OK**	+	Nde		–		–
2	V+ (12–48 V=)	+		–		–	Nde	+	**OK**
3	V_{GND}	–	**OK**	+	Nde	+		–	
4	V+ (12–48 V=)	+		–		–	Nde	+	Nde
5	RxD	–	**Dp [1]**	+	**Dp [1]**	+		–	
6	TxD	+		–		–	**Dp [1]**	+	**Dp [1]**
7	GND	–	Nde	+	Nde	+		–	
8	DO1-1	+		–		–	Nde [2]	+	Nde [2]
9	DO1-2	–	Nde	+	Nde	+		–	
10	DO2-1	+		–		–	Nde [3]	+	Nde [3]
11	DO2-2	–	Nde	+	Nde	+		–	
12	DI1−	+		–		–	**OK [4]**	+	Nde [4]
13	DI1+	–	Nde	+	Nde	+		–	
14	DI2−	+		–		–	**OK [4]**	+	Nde [4]
15	DI2+					+		–	

Explanatory notes for the table:
OK - Normal operation
DP - Damage possible
Nde - No damage expected

[1] - If the applied voltage is > 15 V, damage is likely
[2] - If the relay is closed (normally open), the relay is damaged when current > 5 A
[3] - If the relay is closed (normally closed), the relay is damaged when current > 5 A
[4] - If the applied voltage is > 40 V, input circuit damage is likely

4.2.5. Reset button

The Reset button is placed close to the screw terminal and it is labeled "Reset". Use a blunt tool no more than 1 mm in diameter (e.g. a paper clip) to press the button.

Keep it pressed for at least 3 seconds for reboot and at least 10 seconds for a factory reset. The start of the factory reset is confirmed by all LEDs lighting up for one second. The button can be released afterwards.

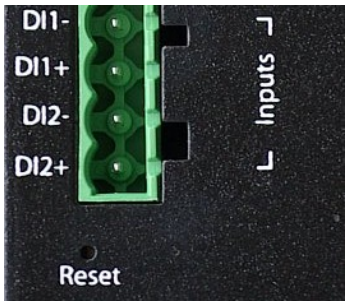


Fig. 4.6: Reset button

4.3. Indication LEDs

Fig. 4.7: Indication LEDs

Tab. 4.7: M!DGE interfaces and status indicators

Label	State	Function
Status	green blinking	Start up, maintenance
	green on	Ready (right side banks description)
	orange on	Ready (left side banks description)
	orange blinking	Insufficient power supply
Connect	blinking	Mobile connection is being established
	on	Mobile connection is up
	green	Excellent GSM signal
	orange	Medium GSM signal
	red	Weak GSM signal
VPN	green on	VPN connection is up
	green blinking	VPN connection is being established
If left side banks displayed		
DO1	on	Closed
	off	Opened
DO2	on	Closed
	off	Opened
DI1	on	Input set
	off	Input not set
DI2	on	Input set
	off	Input not set

4.4. Technical specifications

Tab. 4.8: Technical specifications

Mobile Interface UMTS	WCDMA, HSDPA, HSUPA, HSPA+: bands1, 2, 5, 8 EDGE, GPRS: 850/900/1900 MHz Data rates: max. 14.4 Mbps Downlink / 5.76 Mbps uplink	
Mobile Interface LTE	LTE: bands 1, 2, 3, 5, 7, 8, 20, all bands withs diversity WCDMA, HSPA, HSPA+: bands 1, 2, 3, 5, 8, all bands withs diversity GSM, GPRS, EDGE: 850/900/1800/1900 MHz Data rates up to 100 Mbps downlink / 50 Mbps uplink	
Ethernet	2× Ethernet 10/100 Base-T, Auto MDX, 2× RJ45, bridged or routed	
Serial Interface	1× 3-wire RS232 on 15-pin screw terminal block	
Digital I/O	2 digital inputs	0–5.0 VDC level 0 7.2–40 VDC level 1, maximum voltage 40 VDC
	2 digital outputs	Relay outputs 1st NO, 2nd NC Limiting continuous current 1 A Max. switching voltage 60 VDC, 42 VAC (Vrms) Maximum switching capacity 60 W on 15-pin terminal block
USB service interface	USB host interface supporting memory devices USB type A connector	
Antenna Interface	Impedance:	50 Ω
	Connector:	SMA female
Power Supply	Input voltage:	10.2–57.6 VDC (12–48 VDC −15 % / +20 %)
	Power consumption:	Rx max. 3.2 W Tx max. 5 W
Environmental Conditions	For indoor use only, IP40 Metal casing, DIN rail mounting kit included Temperature range UMTS: −25 to +70 °C (−13 to +158 °F) Temperature range LTE: −25 to +60 °C (−13 to +140 °F) Humidity: 0 to 95 % (non condensing) MTBF (Mean Time Between Failure) > 220.000 hours (> 25 years) Overvoltage Category: II Pollution Degree: 2	
Mounting	DIN rail mounting	
Dimensions / Weight	45 W × 110 D × 125 H mm (1.77 × 4.33 × 4.92 in), ca. 450 g (0.99 lbs)	
Type Approval	CE, FCC	

Options	
Antennas	Various antennas suitable for your application are available
Mounting kit	Flat bracket mounting kit

4.5. Model offerings

M!DGE-UMTS GPRS/EDGE/UMTS/HSPA router, 2Eth, RS232, 2DI, 2DO
DIN rail holder included

M!DGE-LTE GPRS/EDGE/UMTS/HSPA+/LTE router, 2Eth, RS232, 2DI, 2DO
DIN rail holder included

SW feature keys

The SW feature key should be added to a new or running system via adding a license: menu SYSTEM – Licensing (see Section 7.7.7, “Licensing”).

Mobile IP This key allows building a MobileIP VPN tunnel. See http://www.racom.eu/eng/products/m/midge/app/Backup_WAN_by_GSM.html#Mobile_IP_with_VPN_tunnels for short explanation.

Server Ext. OpenVPN server extension - without this key the maximum number of connected clients shall reach 10. This key extends the number to 25.

4.6. Accessories

4.6.1. F bracket

Fig. 4.8: Flat bracket

Flat-bracket

Installation bracket for flat mounting. For usage details see chapter Mounting and chapter Dimensions.

4.6.2. Demo case

A rugged plastic case for carrying up to three RipEX units and one M!DGE 3G SCADA router. It also contains all the accessories needed to perform an on-site signal measurement, complete application bench-test or a functional demonstration of both radio modems and the 3G router. During a field test, units can be powered from the backup battery and the external antenna can be connected to one of the RipEX units through the „N“ connector on the case.

Fig. 4.9: Demo case

Contents:

- Brackets and cabling for installation of three RipEX units and one M!DGE (units not included)
- 1× power supply Mean Well AD-155A (100-240 V AC 50-60 Hz/13.8 V DC)
- 1× Backup battery (12V/5Ah, FASTON.250), e.g. Fiamm 12FGH23
- 1× Power cable (European Schuko CEE 7/7 to IEC 320 C13)
- 1× Ethernet patch cable (3 m, UTP CAT 5E, 2× RJ-45)
- Quick start guide

RipEX accessories:

- 3× Dummy load antennas
- 1× L-bracket, 1x Flat-bracket samples
- 1× Fan kit
- 1× X5 – ETH/USB adapter

M!DGE accessories:

- Whip antenna (900–2100 MHz, 2.2 dBi, vertical)
- External dimensions: 455 × 365 × 185 mm
- Weight approx. 4 kg (excluding RipEXes and M!DGE)

5. Bench test / Step-by-Step guide

Before starting to work with the HW please be sure that you have a SIM card enabled for data and you have all the necessary information from the mobile operator (PIN, APN, login, passwd)

5.1. Connecting the hardware

5.1.1. Install the SIM card

Insert a SIM card into the SIM socket. If the router has two SIM card sockets, use the first one. Make sure the SIM is enabled for data transmission.

There are two reasons for installing the SIM card as the first task: a) the SIM card could be damaged when inserted into the powered equipment, b) the information from SIM card are read only after a power cycle.

5.1.2. Connect the GSM/UMTS antenna

Fit a GSM/UMTS antenna. For details see Section 4.6, “Accessories” or contact RACOM for suitable antennas.

5.1.3. Connect the LAN cable

Connect one M!DGE/MG102i Ethernet port to your computer using an Eth cat.5 cable.

5.1.4. Connect the power supply

Connect the power supply wires to the M!DGE/MG102i screw terminals, ensuring correct polarity. Switch on the power supply.

5.2. Powering up your wireless router

Switch on your power supply. The status LED flashes for a few seconds and after 8 seconds it starts blinking to a green light. After approximately 30 seconds your router will have booted and will be ready; the Status LED remains shining.

When the Mobile Connection is enabled the Connect LED starts blinking while connecting to the GPRS/UMTS network – the color (green/orange/red) represents the signal strength (excellent, medium, weak).

You’ll find the description of the individual LED states in Section 4.3, “Indication LEDs”.

5.3. Connecting M!DGE to a programming PC

a. Please connect the Ethernet interfaces of your computer and M!DGE.
b. If not yet enabled, please enable the Dynamic Host Configuration Protocol (DHCP) so that your computer can lease an IP address from M!DGE. Wait a moment until your PC has received the parameters (IP address, subnet mask, default gateway, DNS server).

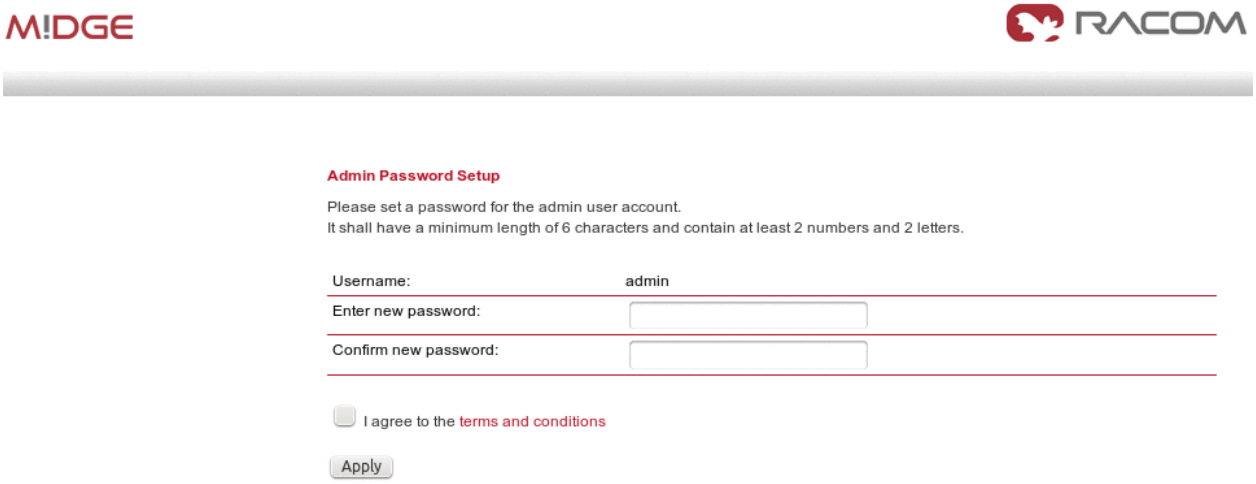
   Alternative: Instead of using the DHCP, configure a static IP address on your PC (e.g. `192.168.1.10` mask `255.255.255.0`) so that it is operating in the same subnet as the M!DGE.

The default IP addresses are:
- `192.168.1.1` for Eth1
- `192.168.2.1` for Eth2

The default subnet mask is `255.255.255.0` for all interfaces.

c. Start a Web Browser on your PC. Type the M!DGE IP address in the address bar:
`http://192.168.1.1`

d. Please set a password for the admin user account. Choose something that is both easy to remember and a strong password (such as one that contains numbers, letters and punctuation). The password must have a minimum length of 6 characters. It must contain a minimum of 2 numbers and 2 letters.


M!DGE
RACOM
Admin Password Setup
Please set a password for the admin user account.
It shall have a minimum length of 6 characters and contain at least 2 numbers and 2 letters.
Username:
admin
Enter new password:
Confirm new password:
I agree to the terms and conditions
Apply

Note

For security reasons, there is no default password.

e. Agree to the terms and conditions. The user is now obliged to accept our end user license agreement during the initial M!DGE setup.

5.4. Basic setup

The M!DGE/MG102i Web Manager can always be reached via the Ethernet interface. After successful setup, Web Manager can also be accessed via the mobile interface. Any up to date web browser can be used. Any web browser supporting JavaScript can be used. By default, the IP address of the Ethernet interface is 192.168.1.1, the web server runs on port 80.

The minimum configuration steps include:

1. Defining the admin password
2. Entering the PIN code for the SIM card
3. Configuring the Access Point Name (APN)
4. Starting the mobile connection

Note

Router (M!DGE or MG102i) can be safely turned off by unplugging the power supply.

6. Installation

6.1. Mounting

M!DGE/MG102i Wireless Router is designed for a DIN rail mounting or on a panel using flat bracket. Please consider the safety instructions in Chapter 10, *Safety, environment, licensing*.

6.2. Antenna mounting

M!DGE/MG102i Wireless Routers will only operate reliably over the GSM network if there is a strong signal. For many applications the flexible stub antenna provided would be suitable but in some circumstances it may be necessary to use a remote antenna with an extended cable to allow the antenna itself to be positioned so as to provide the best possible signal reception. RACOM can supply a range of suitable antennas.

Beware of the deflective effects caused by large metal surfaces (elevators, machine housings, etc.), close meshed iron constructions and choose the antenna location accordingly. Fit the antenna or connect the antenna cable to the GSM antenna connector.

In external antennas the surge protection of coaxial connection would be required.

Note

Be sure that the antenna was installed according to the recommendation by the antenna producer and all parts of the antenna and antenna holder are properly fastened.

6.3. Grounding

Grounding screw has to be properly connected with cabinet grounding using a copper wire with minimal cross section of 4 mm^2.

Fig. 6.1: Grounding

6.4. Power supply

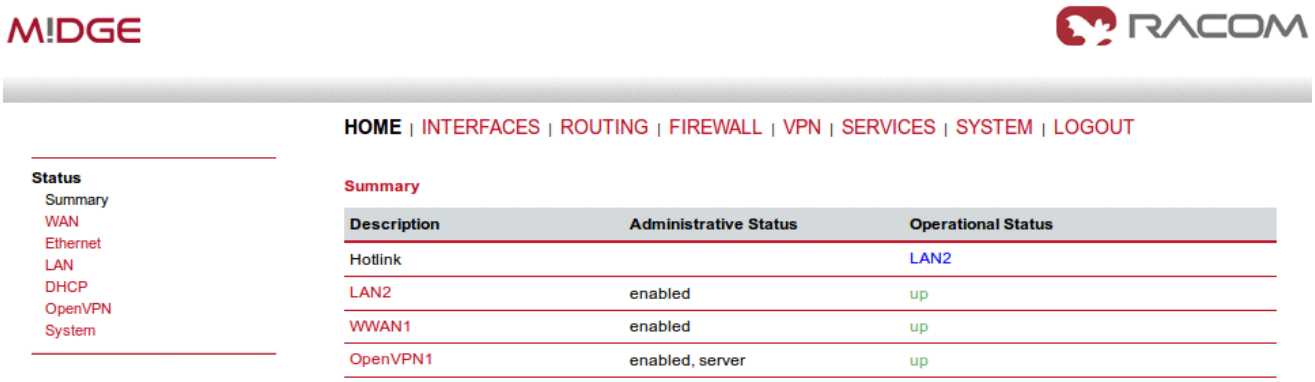
M!DGE can be powered with an external power source capable of voltages from 10 to 55 Volts DC. M!DGE should be powered using a certified (CSA or equivalent) power supply, which must have a limited and SELV circuit output.

M!DGE is equipped with dual power supply connector - it is possible to use two independent power supplies (even with different voltage). The ground terminals are connected together and they are connected with the box grounding as well.

7. Web Configuration

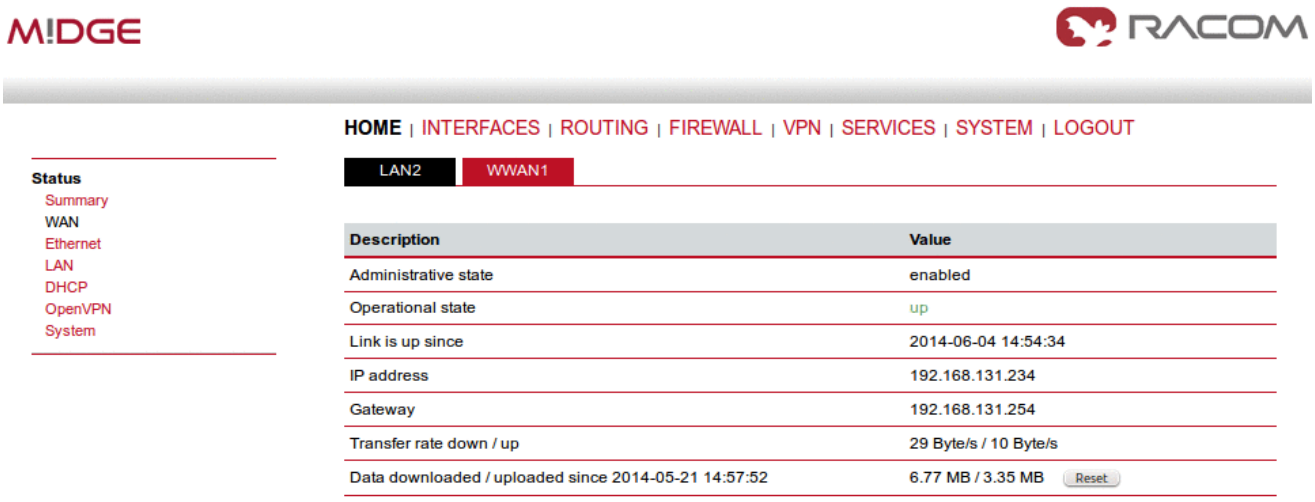
7.1. HOME

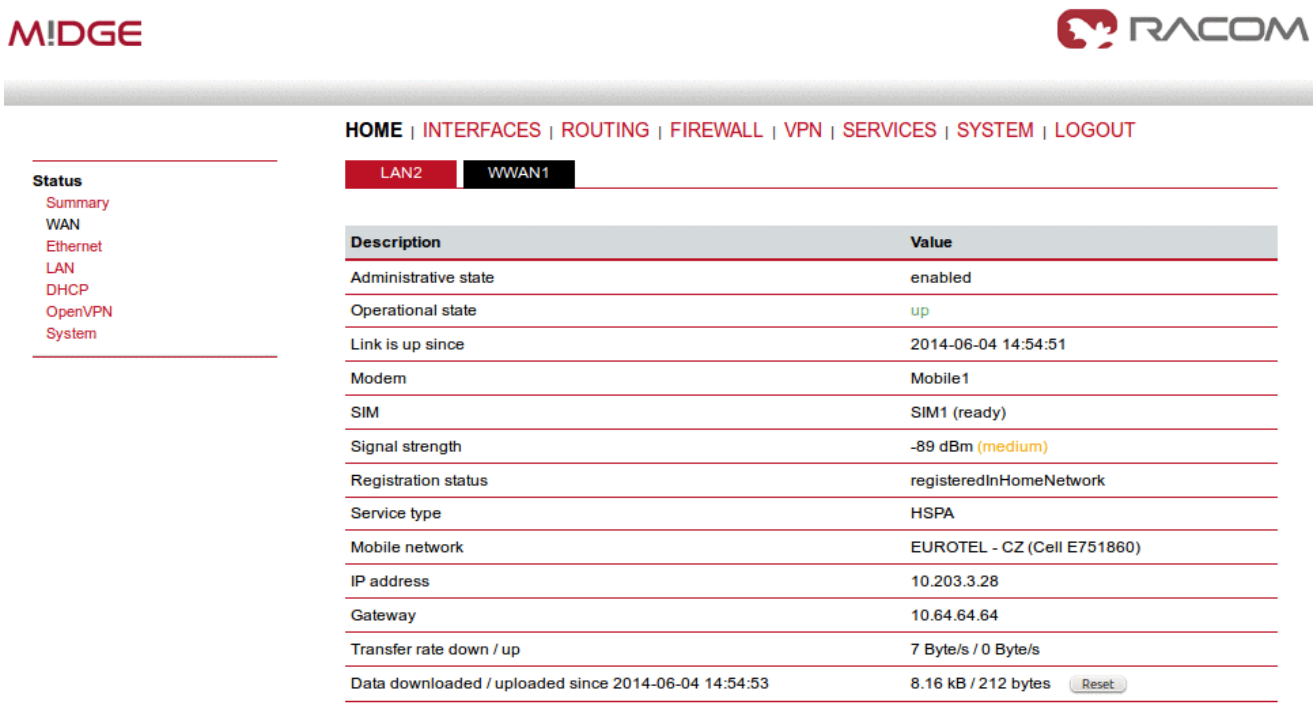
This page gives you a system overview. It helps you when initially setting up the device and also functions as a dashboard during normal operation.



The highest priority link which has been established successfully will become the so-called **hotlink** which holds the default route for outgoing packets.

Detailed information about status of each WAN interface is available in a separate window.





7.2. INTERFACES

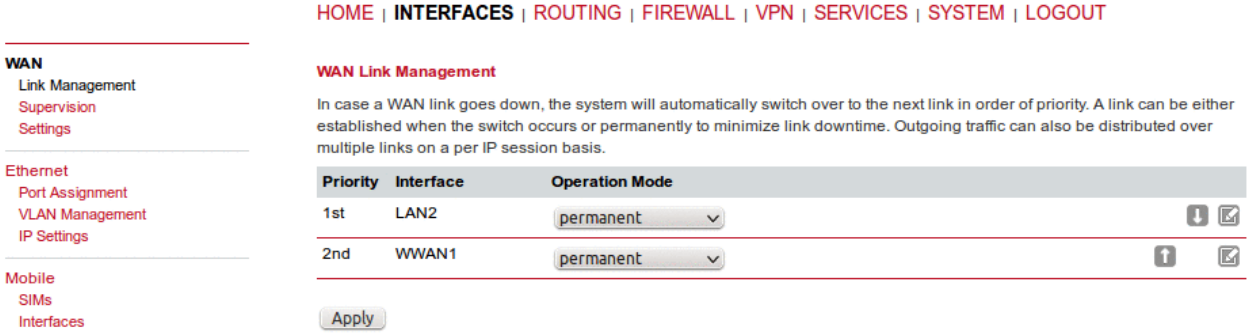
Details for all physical connections are given in Section 4.2, “Connectors”.

7.2.1. WAN

Link Management

Each available item in the WAN Link Manager matches with the particular WAN interface - for adding an item, the respective WAN interface must be set (e.g. LAN, WWAN).

In case a WAN link goes down, the system will automatically switch over to the next link in order of priority (the priorities can be changed using the arrows on the right side of the window). A link can be either established when the switch occurs or permanently to minimize link downtime.


HOME | INTERFACES | ROUTING | FIREWALL | VPN | SERVICES | SYSTEM | LOGOUT
WAN
Link Management
Supervision
Settings
Ethernet
Port Assignment
VLAN Management
IP Settings
Mobile
SIMs
Interfaces
WAN Link Management
In case a WAN link goes down, the system will automatically switch over to the next link in order of priority. A link can be either established when the switch occurs or permanently to minimize link downtime. Outgoing traffic can also be distributed over multiple links on a per IP session basis.
Priority
Interface
Operation Mode
1st
LAN2
permanent
2nd
WWAN1
permanent
Apply

1st priority: This link will be used whenever possible.

2nd priority: The first fallback technology.

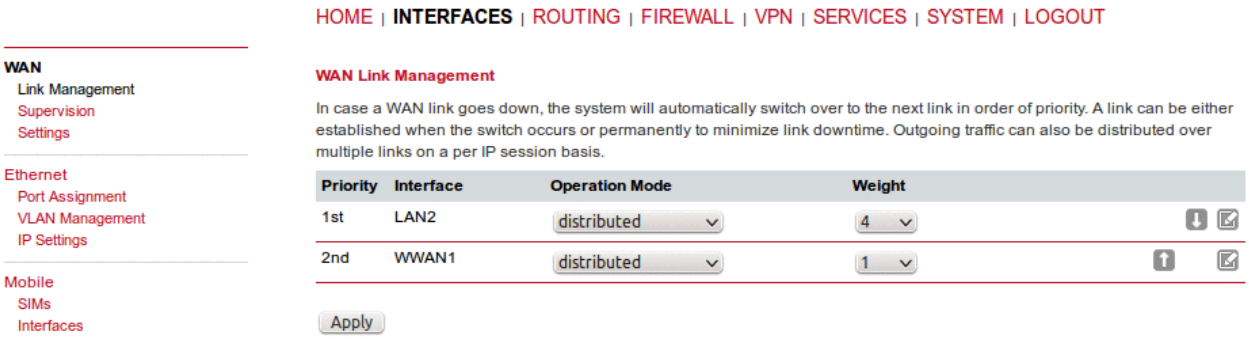
Up to four priorities can be used.

Outgoing traffic can also be distributed over multiple links on a per IP session basis. Choose the option "distributed" as an Operation Mode with the appropriate Weight.

In the following example, the outgoing traffic will be distributed between LAN2 (80 %) and WWAN1 (20 %) links.

Note

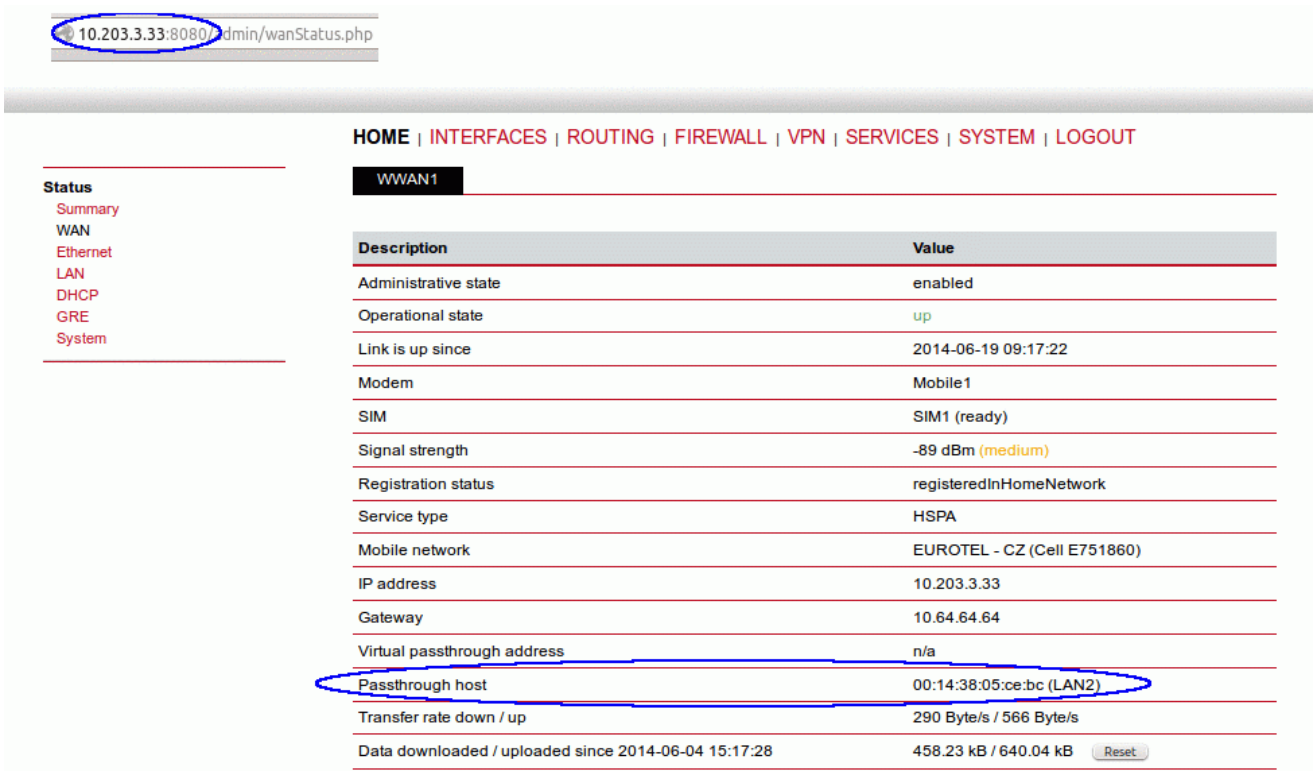
This option is general and applies to all outgoing traffic. See section 7.3.3 Multiple Routes for more detailed configuration.



We recommend using the **permanent** option for WAN links. However, in case of time-limited mobile tariffs, the **switchover** option should be used.

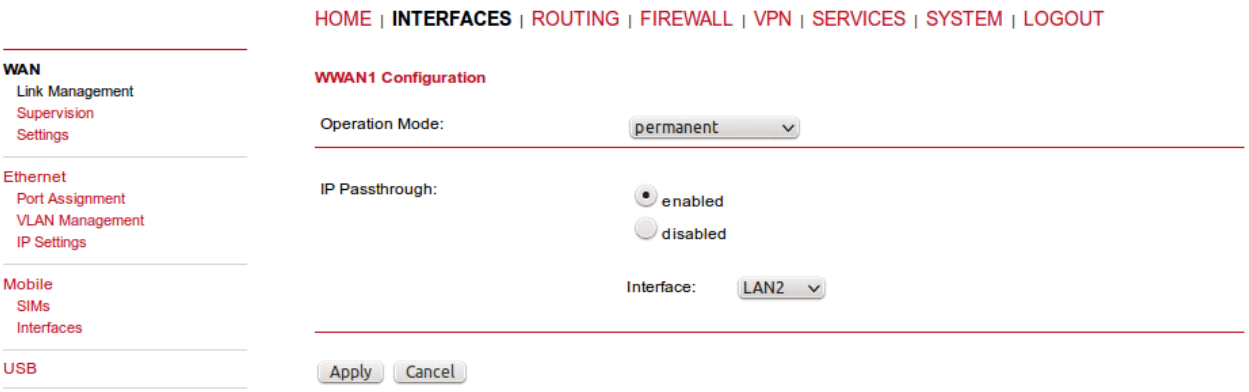
After clicking on the WWAN "Edit" button, you can additionally set the "IP passthrough" option for the LAN2 interface. The result is that the connected device over the LAN2 port will obtain M!DGE's/MG102i's mobile IP address via DHCP. In another words, M!DGE/MG102i will be transparent for the connected device and will only serve for the mobile connectivity. Typically, such connected device (e.g. firewall) will not need any special configuration facing M!DGE/MG102i, it will just use its mobile IP address (usually the public IP address).

Once established, the Web manager can be reached over the port 8080 using the public address.

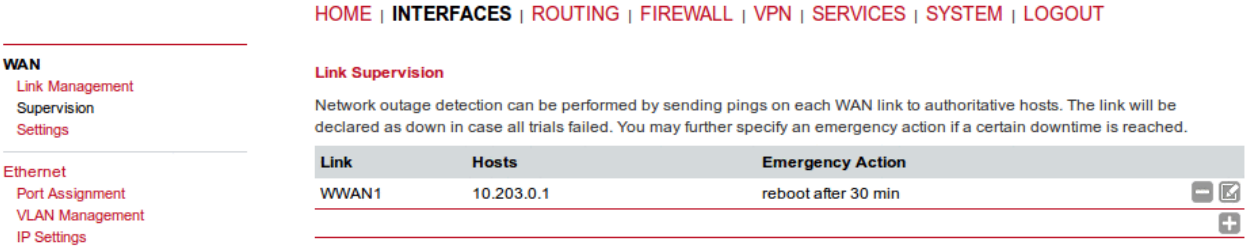


Note

- This option is configurable within WWAN links only. Remember that LAN1 cannot be used as the port for the IP passthrough functionality.
- LAN10 is not usable within M!DGE/MG102i routers. Do not select it.



Connection Supervision

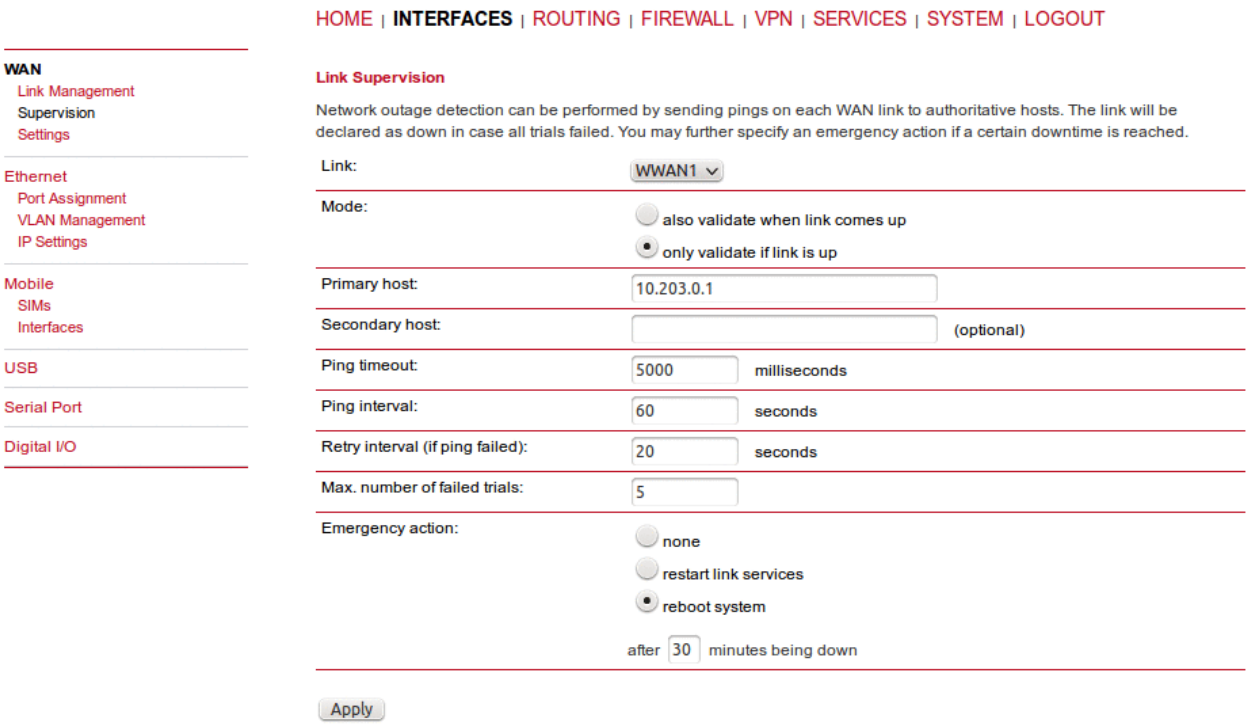

HOME | INTERFACES | ROUTING | FIREWALL | VPN | SERVICES | SYSTEM | LOGOUT
WAN
Link Management
Supervision
Settings
Ethernet
Port Assignment
VLAN Management
IP Settings
Link Supervision
Network outage detection can be performed by sending pings on each WAN link to authoritative hosts. The link will be declared as down in case all trials failed. You may further specify an emergency action if a certain downtime is reached.
Link
Hosts
Emergency Action
WWAN1
10.203.0.1
reboot after 30 min

Network outage detection can be used for switching between available WAN links and can be performed by sending pings on each link to authoritative hosts. A link will be declared as down if all trials have failed. The link will be considered up again if at least one host is reachable.

You may further specify an emergency action if no uplink can be established at all.

Configurable actions are:

- None
- Restart link services
- Reboot system



Link: The WAN link to be monitored (can be ANY for all configured links).

Mode: Specifies whether the link is monitored during the connection establishment or only when it is already up.

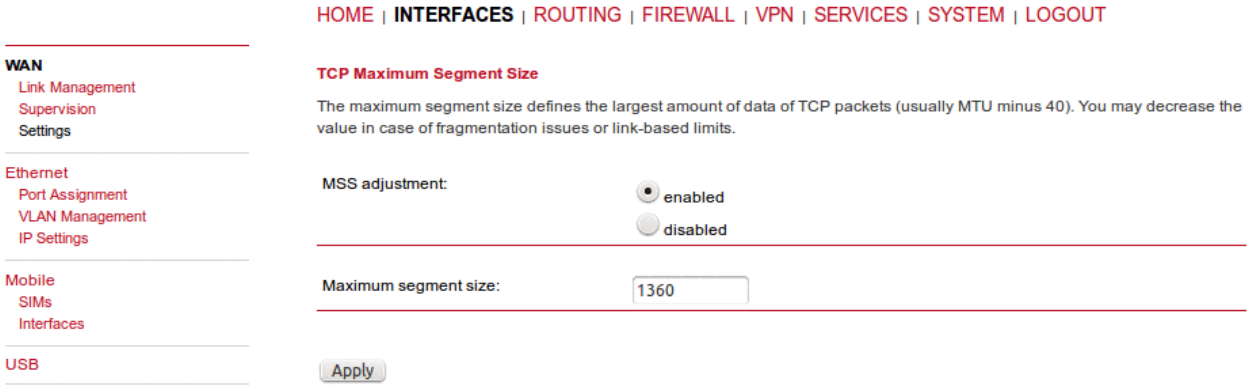
Primary host: Reference host one which will be used for checking IP connectivity (via ICMP pings).

Secondary host: Reference host two which will be used for checking IP connectivity (via ICMP pings). The test is considered successful if either the primary or the secondary host answers.

Ping timeout: Time for which the system is waiting for the ping response. With mobile networks the response time can be quite long (several seconds) in special cases. You can check the typical response using SYSTEM – Troubleshooting – Network Debugging – Ping. The first response typically takes a longer time than the following ones in GPRS/UMTS networks, the Ping timeout should be set to the longer time than with the first response.

Ping interval:	Time to wait before sending the next probe.
Retry interval (if ping failed):	If the first trial fails, ping hosts in this modified interval until the ping is successful or the maximum number of failed trials is reached.
Max. number of failed trials:	The maximum number of failed ping trials until the ping check will be declared as failed.
Emergency action:	Configure the Emergency action which should be taken after the maximum downtime is reached. Using "reboot" perfoms the system reboot. The option "restart services" restarts all link-related applications including the modem reset. No action is done if the "none" option is set. Configure the maximum amount of downtime in minutes for which the link could not be established.

Settings



The maximum segment size defines the largest amount of data of TCP packets (usually MTU minus 40). You may decrease the value in case of fragmentation issues or link-based limits.

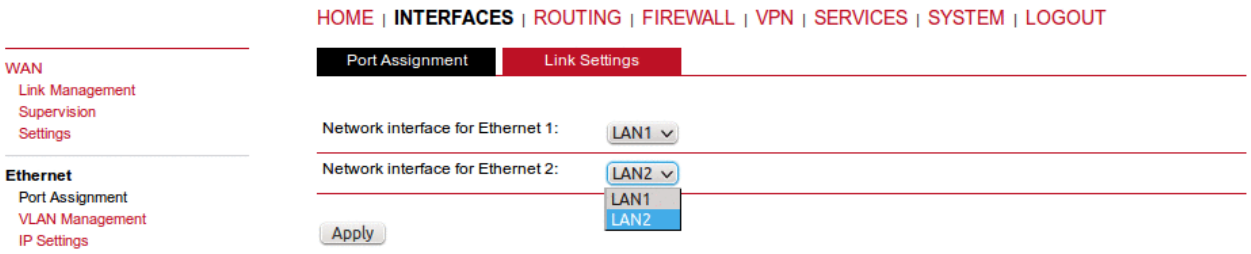
MSS adjustment	Enable or disable MSS adjustment on WAN interfaces.
Maximum segment size	Maximum number of bytes in a TCP data segment.

7.2.2. Ethernet

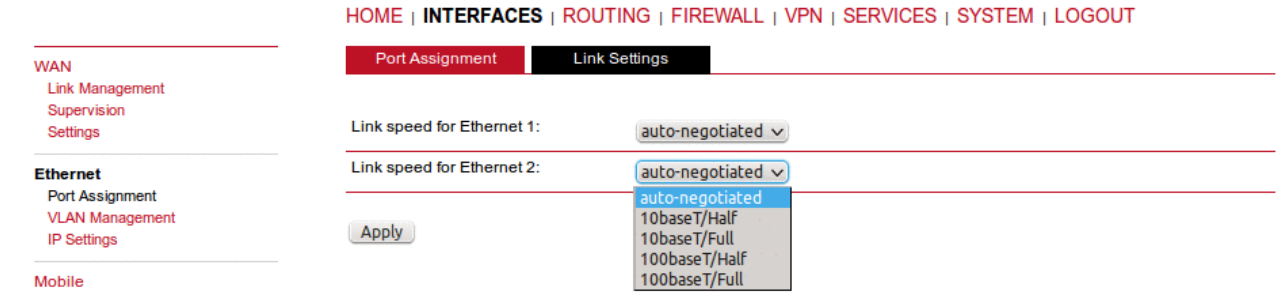
Port Assignment

This menu can be used to individual assigning of Ethernet ports to LAN interfaces if you want to have different subnets per port or to use one port as the WAN inteface.

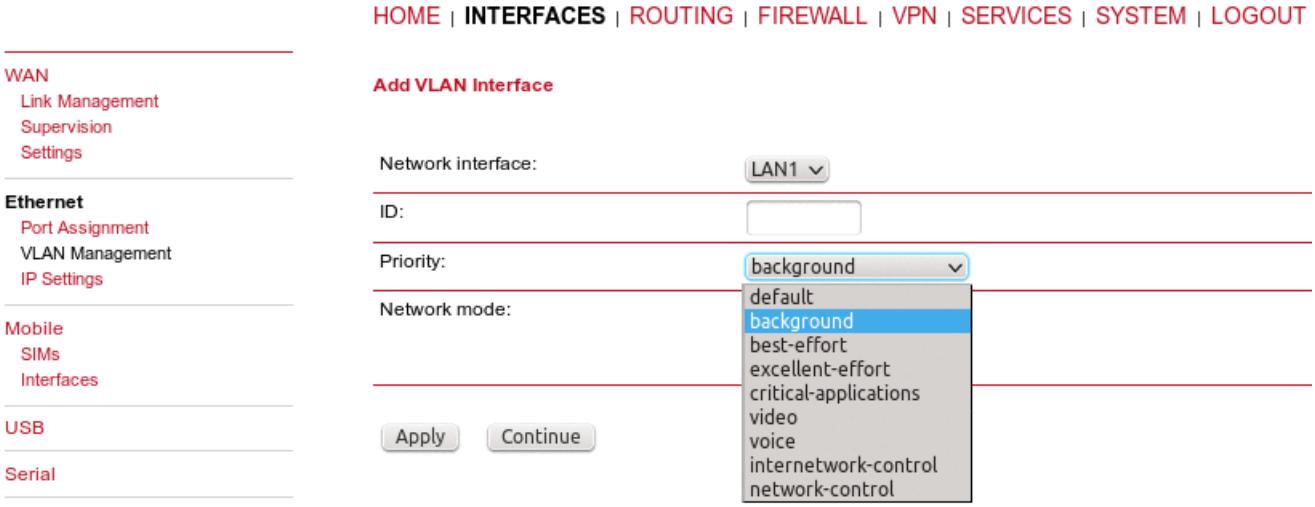
If it is desired to have both ports in the same LAN you may assign them to the same interface. Please note that the ports will be bridged by software and operated by running the Spanning Tree Protocol.



Link negotiation can be set for each Ethernet port individually. Most devices support auto-negotiation which will configure the link speed automatically according to the existing devices in the network, however manual setting of 10 BaseT or 100 BaseT and Half or Full duplex can be set as well.



VLAN Management



M!DGE/MG102i routers support Virtual LAN according to IEEE 802.1Q which can be used to create virtual interfaces on top of the Ethernet interface. The VLAN protocol inserts an additional header to Ethernet frames carrying a VLAN Identifier (VLAN ID) which is used for distributing the packets to the associated virtual interface. Any untagged packets, as well as packets with an unassigned ID, will be distributed to the native interface. In order to form a distinctive subnet, the network interface of a remote LAN host must be configured with the same VLAN ID as defined on the router. Further, 802.1P introduces a priority field which influences packet scheduling in the TCP/IP stack.

The following priority levels (from the lowest to the highest) exist:

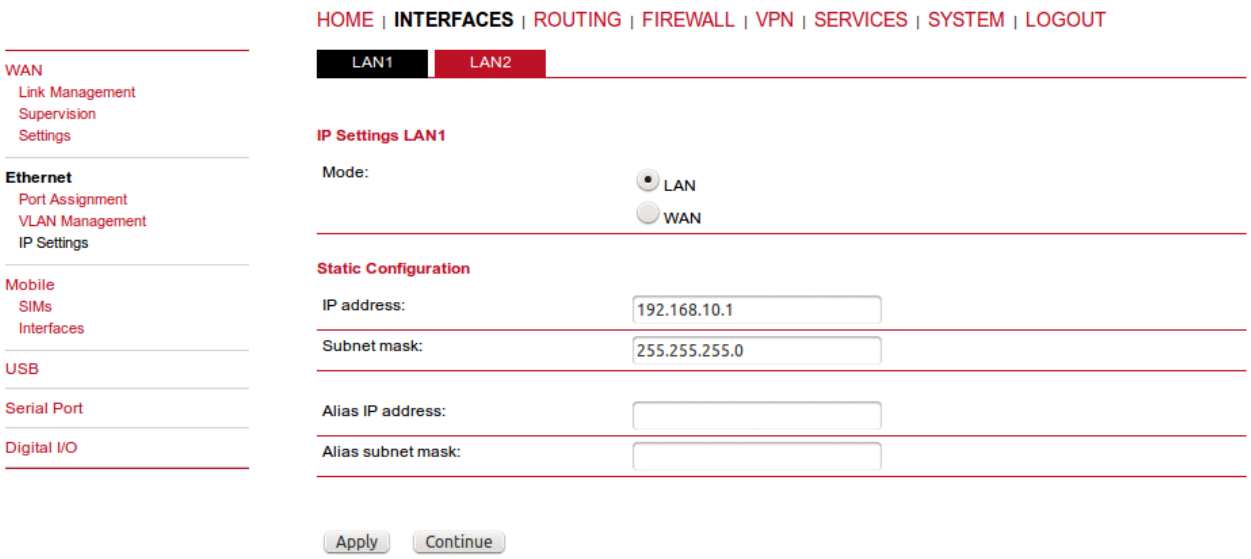
Parameter	VLAN Priority Levels
0	Background
1	Best Effort
2	Excellent Effort
3	Critical Applications
4	Video (< 100 ms latency and jitter)
5	Voice (< 10 ms latency and jitter)
6	Internetwork Control
7	Network Control

IP Settings

Two individual tabs will be used when different LANs are set in the Port settings menu. Each of them can be configured either in the LAN mode or in the WAN mode.

Note

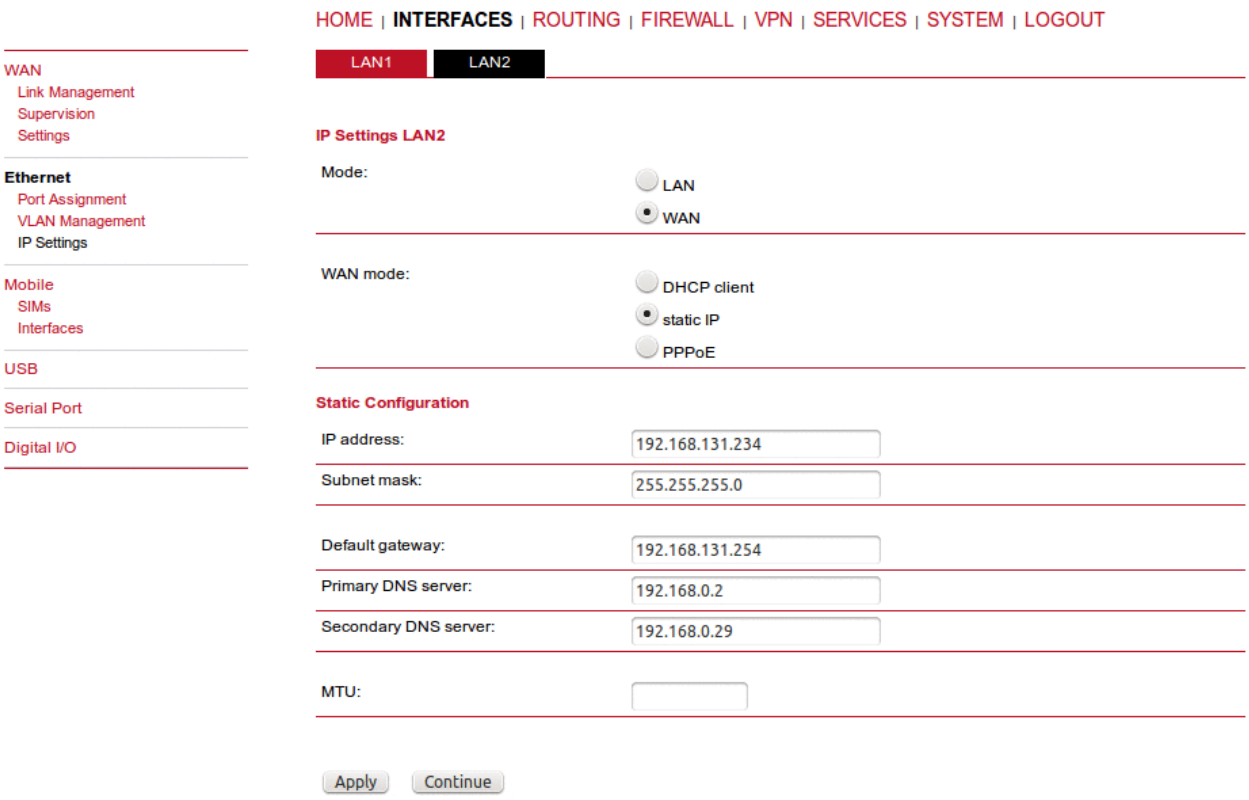
The default IP addresses are as follows: 192.168.1.1/24 (LAN1) and 192.168.2.1/24 (LAN2).



Static configuration of M!DGE's/MG102i's own IP address and Subnet mask is available for the LAN mode. The Alias IP address enables configuring the LAN inteface with a second IP address/subnet.

Note

Setting of the IP address is interconnected with the DHCP Server (if enabled) - menu the SERVICES - DHCP Server menu.



WAN mode enables the following possibilities:

DHCP client: The IP configuration will be retrieved from a DHCP server in the network. No further configuration is required (you may only set MTU).

Static IP: IP configuration will be set manually. At least the Default gateway and the Primary DNS server must be configured along with the IP address and subnet mask.

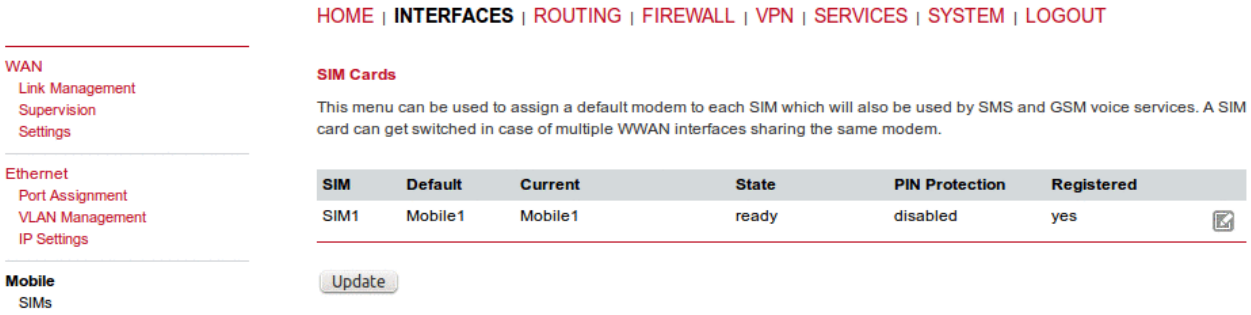
PPPoE: PPPoE is the preferred protocol when communicating with another WAN access device (like a DSL modem).

- Username: PPPoE user name to be used for authentication at the access device.
- Password: PPPoE password to be used for authentication at the access device.
- Service Name: Specifies the service name set of the access concentrator. Leave it blank unless you have many services and need to specify the one you need to connect to.
- Access Concentrator Name: This may be left blank and the client will connect to any access concentrator.

7.2.3. Mobile

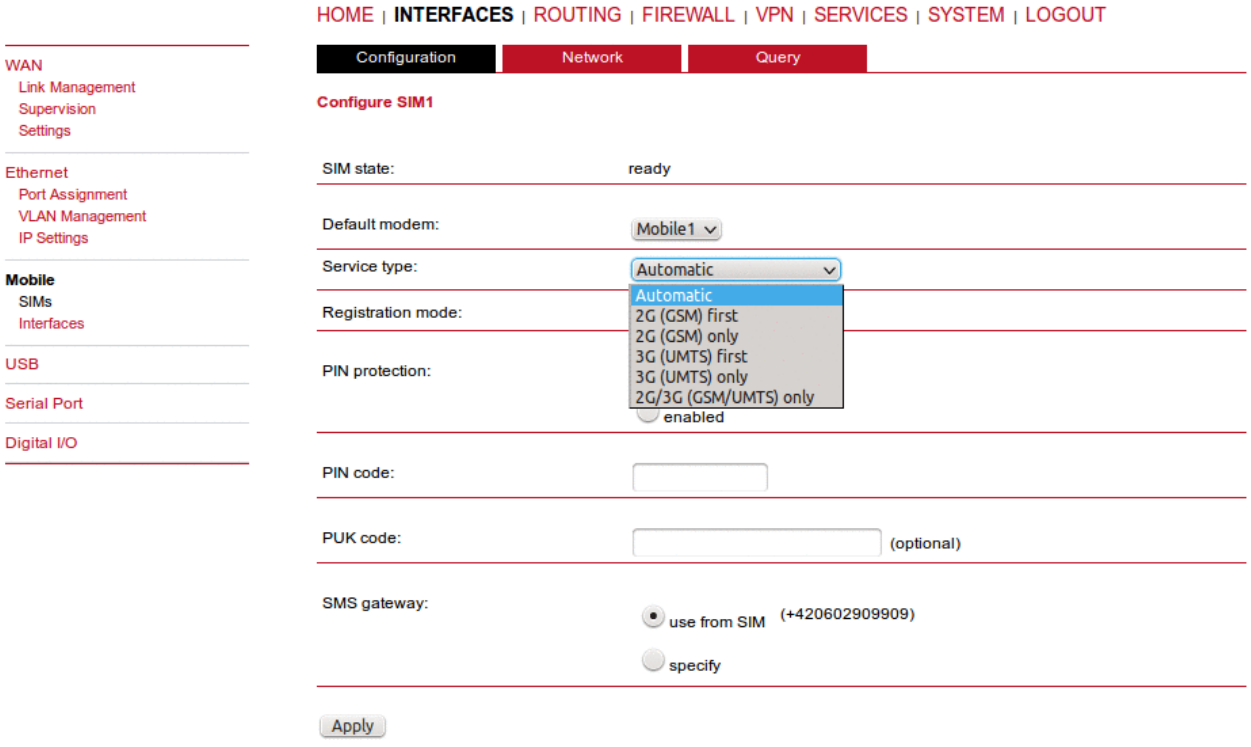
SIMs

The SIM page gives an overview about the available SIM cards, their assigned modems and the current states. Once a SIM card has been inserted, assigned to a modem and successfully unlocked, the card should remain in the ready and registered state. You may update the state in order to restart PIN unlocking and trigger another network registration attempt.



Configuration

A SIM card is generally assigned to a default modem but this may switch, for instance if you set up two WWAN interfaces with one modem but different SIM cards. Close attention has to be paid when other services (such as SMS or Voice) are operating on that modem as a SIM switch will affect their operation.



You can configure the following parameters:

Default modem	The default modem assigned to this SIM card.
Service type	The default service type to be used with this SIM card. Remember that the link manager might change this in case of different settings. The default option is "automatic", in areas with interfering base stations you can force a specific

	type (e.g. 3G-only) in order to prevent any flapping between the stations around.
Registration mode	The default option is set to "all networks". You can limit the modem registration to "packet-switched only" (e.g. no Dial-in Server) or "circuit-switched only" option, which can be for example used for the Dial-in Server so one can use PPP over the Circuit-Switched Networks (analog modem style).
PIN protection	Depending on the used card, it can be necessary to unlock the SIM with a PIN code. Please check the account details associated with your SIM whether the PIN protection is enabled.
PIN code	The PIN code for unlocking the SIM card
PUK code	The PUK code for unlocking the SIM card if the card was blocked due to several wrong PIN attempts.
SMS gateway	The service center number for sending short messages. It is generally retrieved automatically from your SIM card but you may define a fixed number here.

Network

This page provides you with the information about the current network status, service type, signal strength, CID (Cell ID), LAC (Local Area Code) and LAI (Local Area Identifier) to which the modem has been registered. LAI is a globally unique number that identifies the country, network provider and LAC of any given location area. It can be used to force the modem to register to a particular mobile cell in case of competing stations.

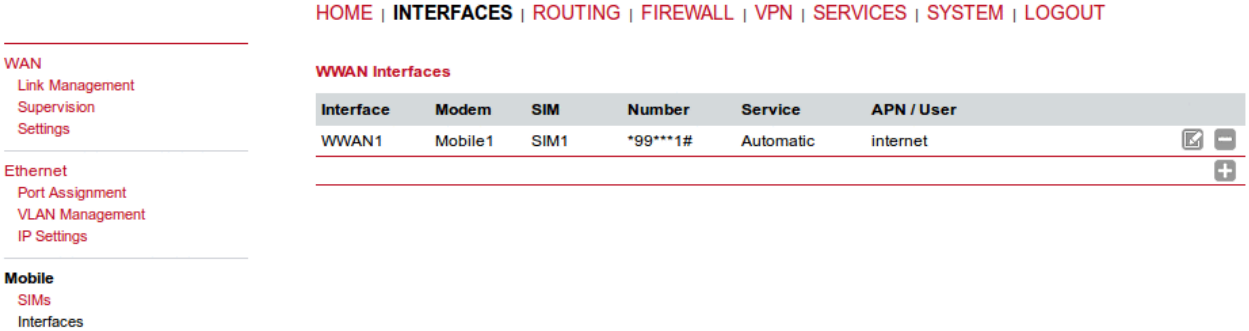
You may further initiate mobile network scan for getting networks in range and assign a LAI manually.

Query

This page allows you to send a Hayes AT command to the modem. Besides the 3GPP-conforming AT command set, further modem-specific commands can be applied which can be provided on demand. Some modems also support to run Unstructured Supplementary Service Data (USSD) requests, e.g. for querying the available balance of a pre-paid account.

WWAN Interfaces

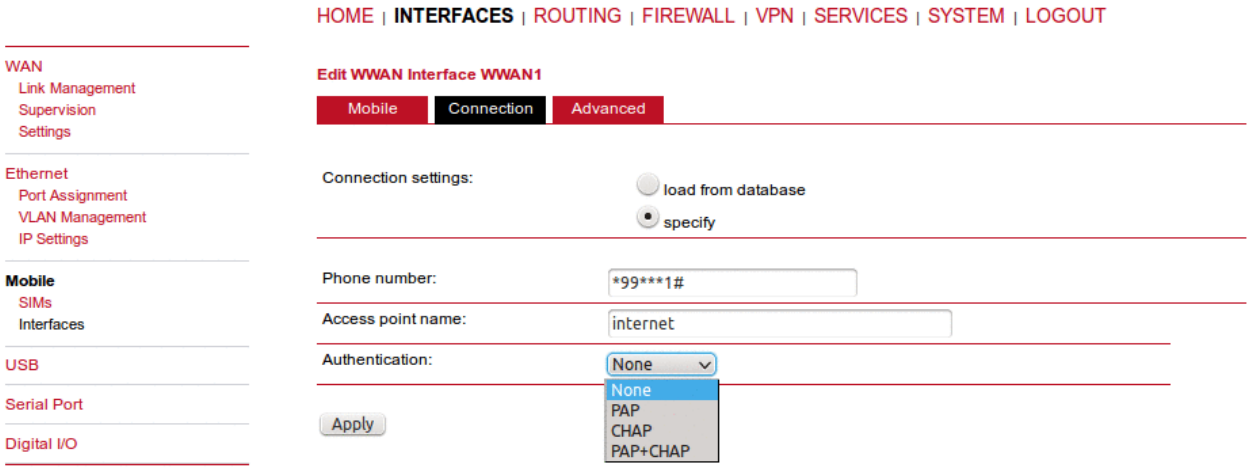
This page can be used to manage your WWAN interfaces. The resulting link will pop up automatically on the WAN Link Management page once an interface has been added. The Mobile LED will be blinking during the connection establishment process and goes on as soon as the connection is up. Refer to the troubleshooting section or log files in case the connection did not come up.



The following mobile settings are required:

Modem	The modem to be used for this WWAN interface
SIM	The SIM card to be used for this WWAN interface
Service type	The required service type

Please note that these settings supersede the general SIM based settings as soon as the link is being dialed.



Generally, the connection settings are derived automatically as soon as the modem has been registered and the network provider has been found in our database. Otherwise, it will be required to configure the following settings:

Phone number	The phone number to be dialed, for 3G+ connections this commonly refers to be *99***1#. For circuit switched 2G connections you can enter the fixed phone number to be dialed in the international format (e.g. +420xx).
Access point name	The access point name (APN) being used
Authentication	The authentication scheme being used, if required this can be PAP or/and CHAP
Username	The username used for authentication
Password	The password used for authentication

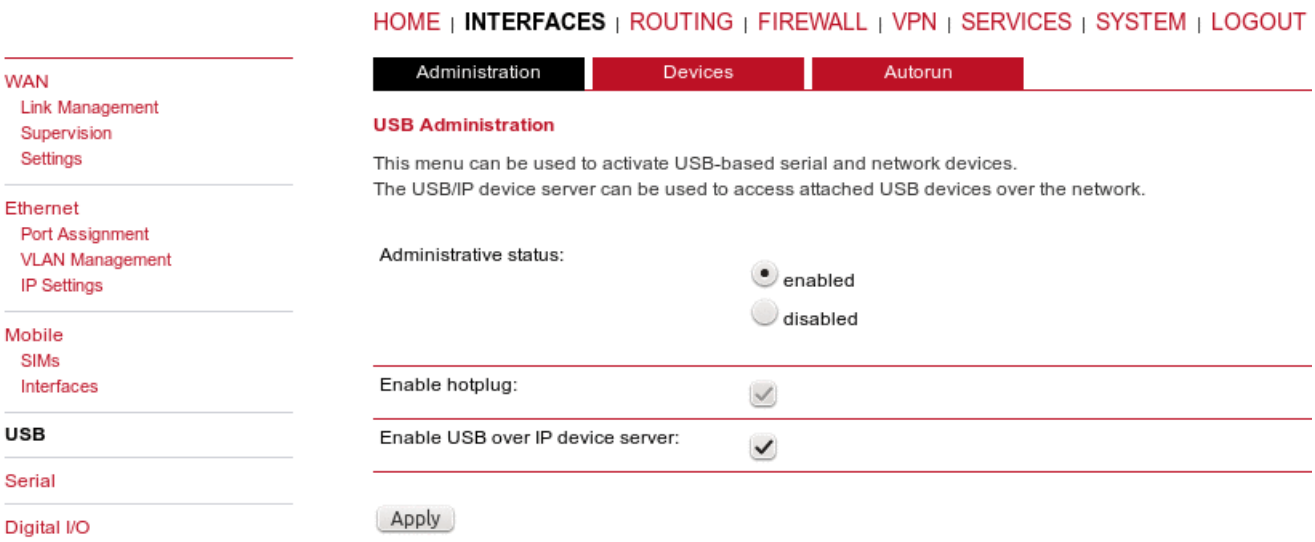
Further on, you may configure the following advanced settings:

Required signal strength	The minimum required signal strength before the connection is dialed.
Home network only	Determines whether the connection should only be dialed when registered to the home network.
Negotiate DNS	Specifies whether the DNS negotiation should be performed and the retrieved name-servers should be applied to the system.
Call to ISDN	This option must be enabled in case of 2G connections talking to an ISDN modem.

Header compression	Enables or disables Van Jacobson TCP/IP Header Compression for PPP-based connections. This feature will improve TCP/IP performance over slow serial links. Has to be supported by your provider.
Data compression	Enables or disables the data compression for PPP-based connections. Data compression reduces the packet size to improve throughput. Has to be supported by your provider.
Client address	Specifies a fixed client IP address on the mobile interface.
MTU	The Maximum Transmission Unit represents the largest amount of data that can be transmitted within one IP packet and can be defined for any WAN interface.

7.2.4. USB

Administration



Enable or disable the USB administration. If enabled, any supported USB converter can be attached and configured for example as another serial link (RS232, see Section 7.2.5, “Serial Port”).

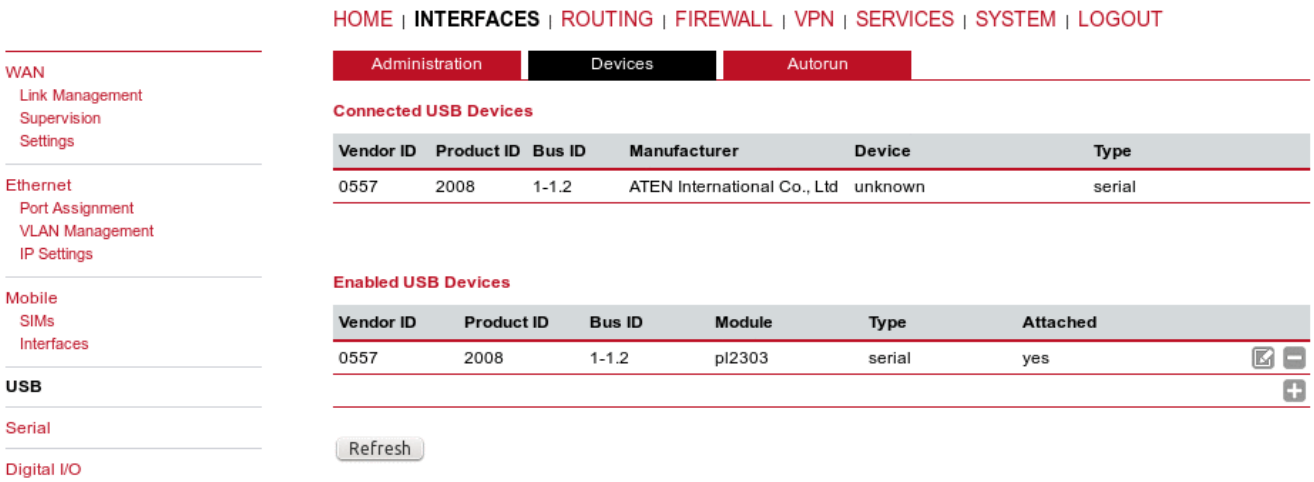
Note

Supported modules are pl2303, ch341 and ftdi (quad-channel adapter).

Following parameters can be configured:

- **Enable hotplug (always enabled)**
- **Enable USB/IP device server**
  The USB/IP Device server can be used for the communication between the unit and the USB device via IP. This is being accomplished by tunneling the USB protocol over IP. The required USB/IP enumerator (Windows application) for accessing the USB stick from the computer can be provided to you on demand.

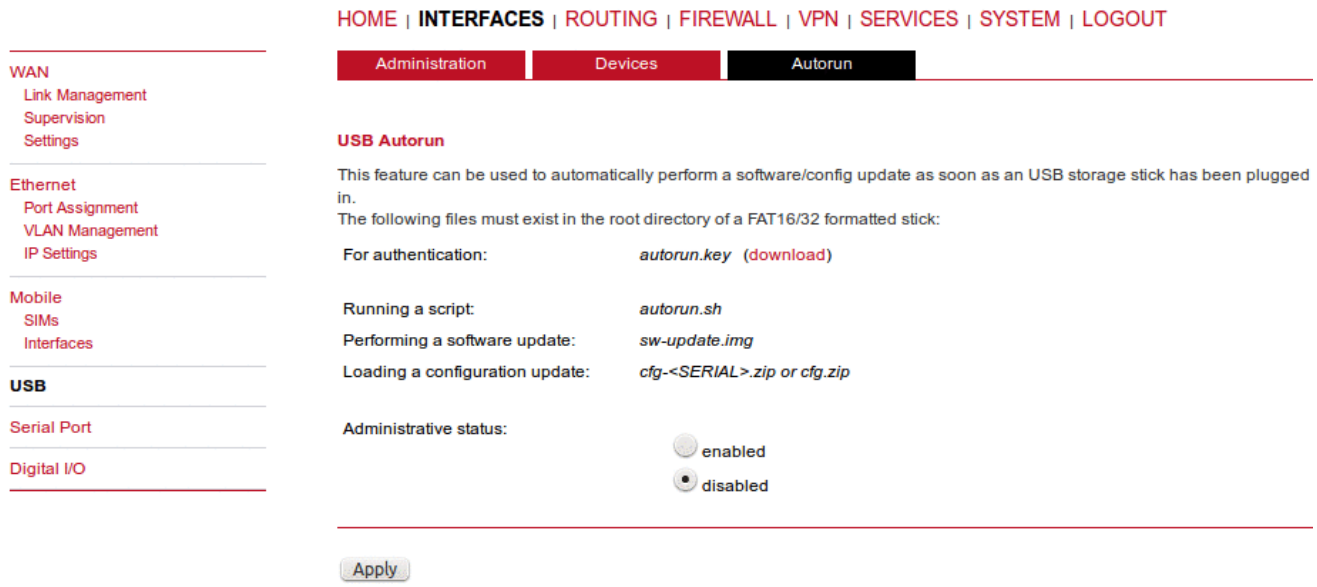
Click on the Refresh button in the tab Devices for displaying connected USB devices and add them with by clicking on the plus sign.



Autorun

This feature can be used to automatically perform a software/config update as soon as an USB storage stick has been plugged in. Following files must exist in the root directory of a FAT16/32 formatted stick:

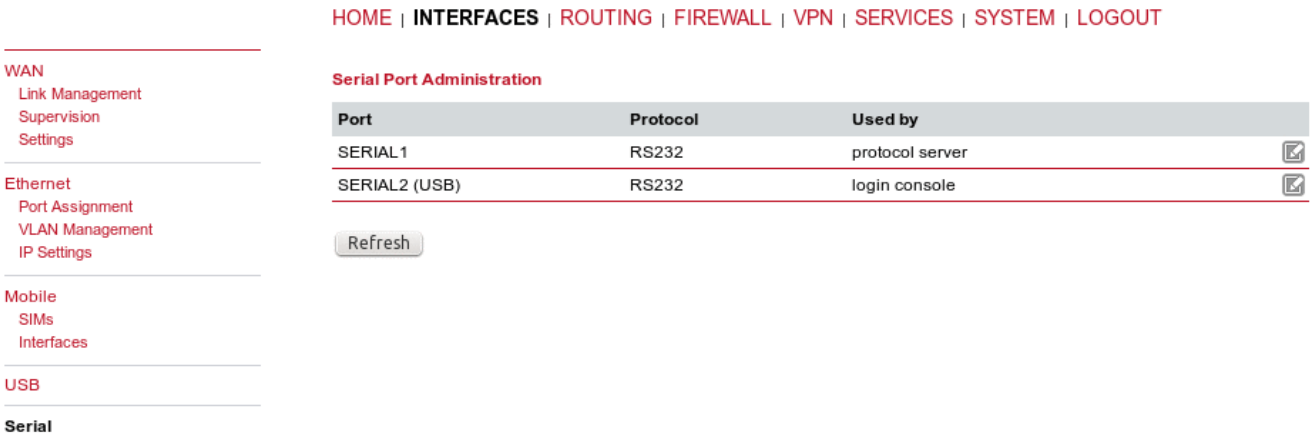
- For authentication: `autorun.key`
- For a software update: `sw-update.img`
- For a configuration update: `cfg-<SERIALNO>.zip` or `cfg.zip`



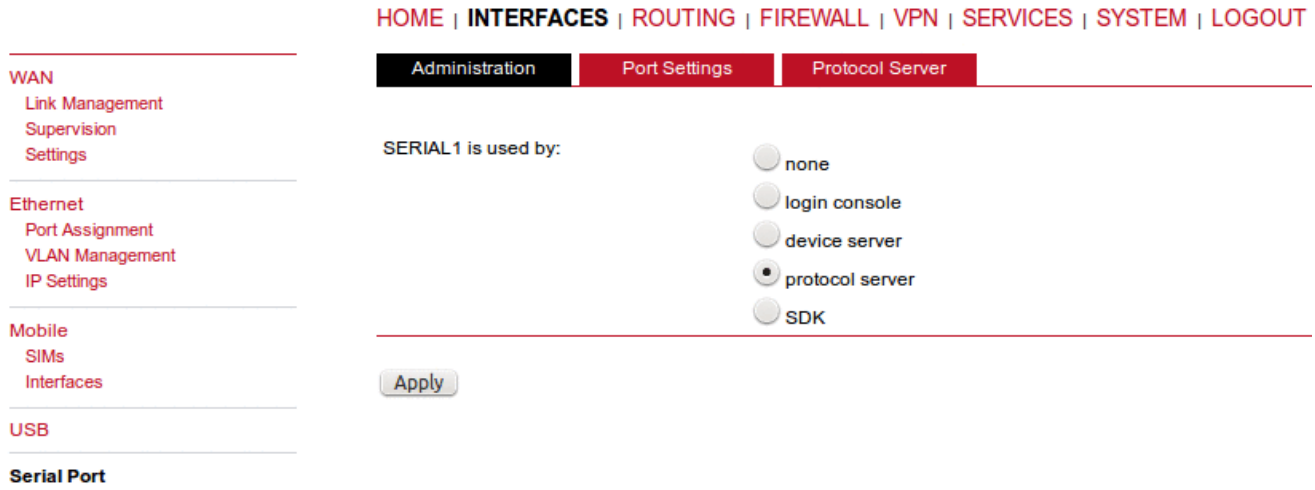
Enable auto run feature: Enable or disable auto run feature.

The `autorun.key` file must hold valid access keys to perform any actions when the storage device is plugged in. The keys are made up of your admin password. They can be generated and downloaded. You may also define multiple keys in this file (line-after-line) in case your admin password differs if applied to multiple M!DGE/MG102i routers.

7.2.5. Serial Port



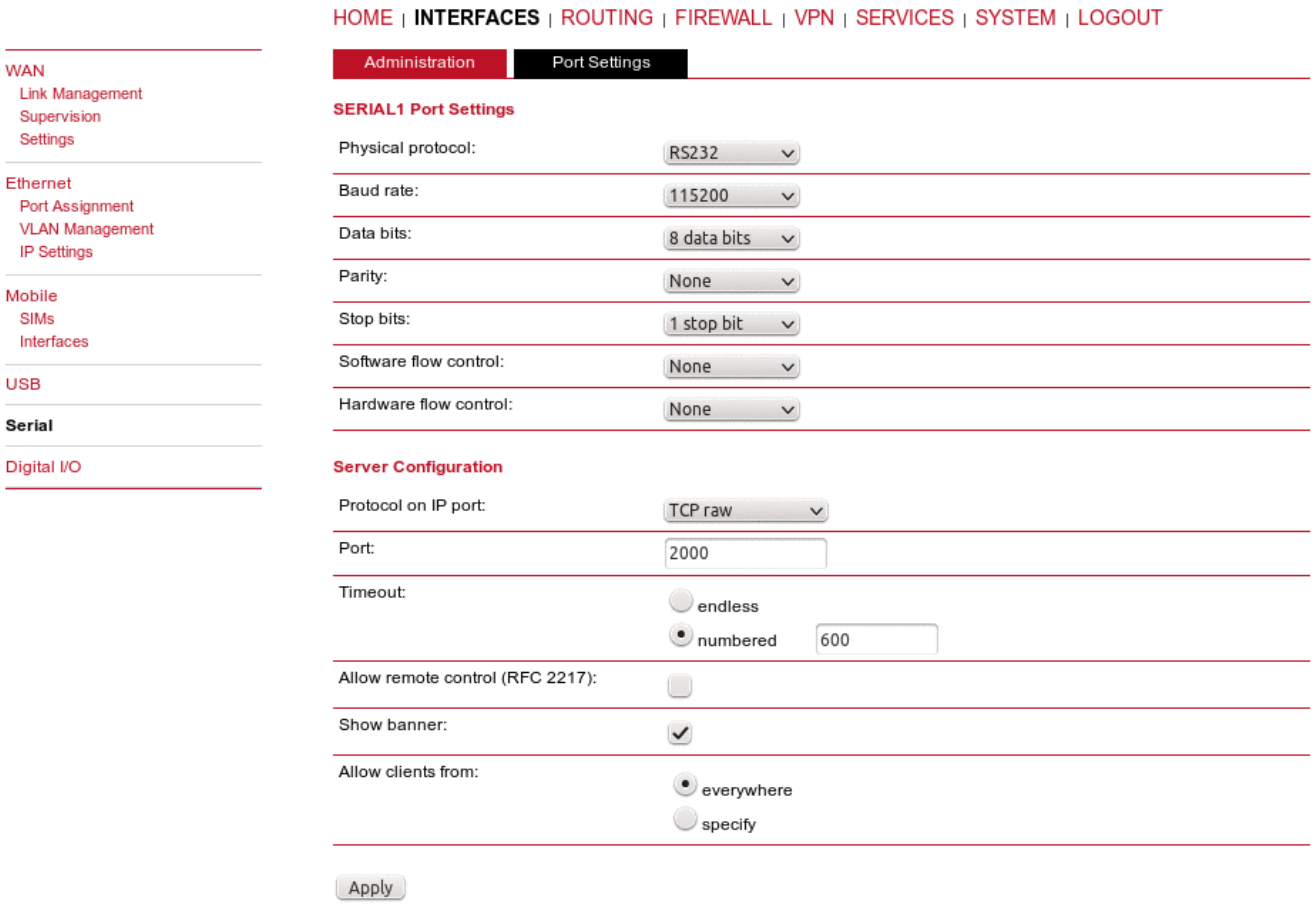
The serial protocol can function in various ways, configure it using the Edit button on the right. If the USB Administration is enabled, an extra SERIAL2 (USB) is available.



Five possibilities are available:

None	The serial port is not used at all.
Login console	A possibility to control the unit via the CLI commands when connected to the serial port (115200 8N1). There are no extra configuration parameters.
Device server	Use this option to control the serial device via IP (transmit the data over the cellular network, ...). See the details below.
Protocol server	Special implementation of various serial protocols like Modbus, IEC101, DNP3, ... See the details below.
SDK	This option enables controlling the serial interface via the SDK scripts (similar to C programming). See chapter SDK for more details.

Device Server



Serial Port Settings: Configure the required RS232 parameters.

Physical protocol:	Only RS232 is supported.
Baud rate:	Specifies the baud rate of the COM port.
Data bits:	Specifies the number of data bits contained in each frame.
Parity:	Specifies the parity used with every frame that is transmitted or received.
Stop bits:	Specifies the number of stop bits used to indicate the end of a frame.
Software flow control:	In XON/XOFF software flow control, either end can send a stop (XOFF) or start (XON) character to the other end to control the rate of incoming data.
Hardware flow control:	While 3 wired connection is used with M!DGE/MG102i hardware flow control is not available.

Server Configuration: “Telnet” or “TCP raw”

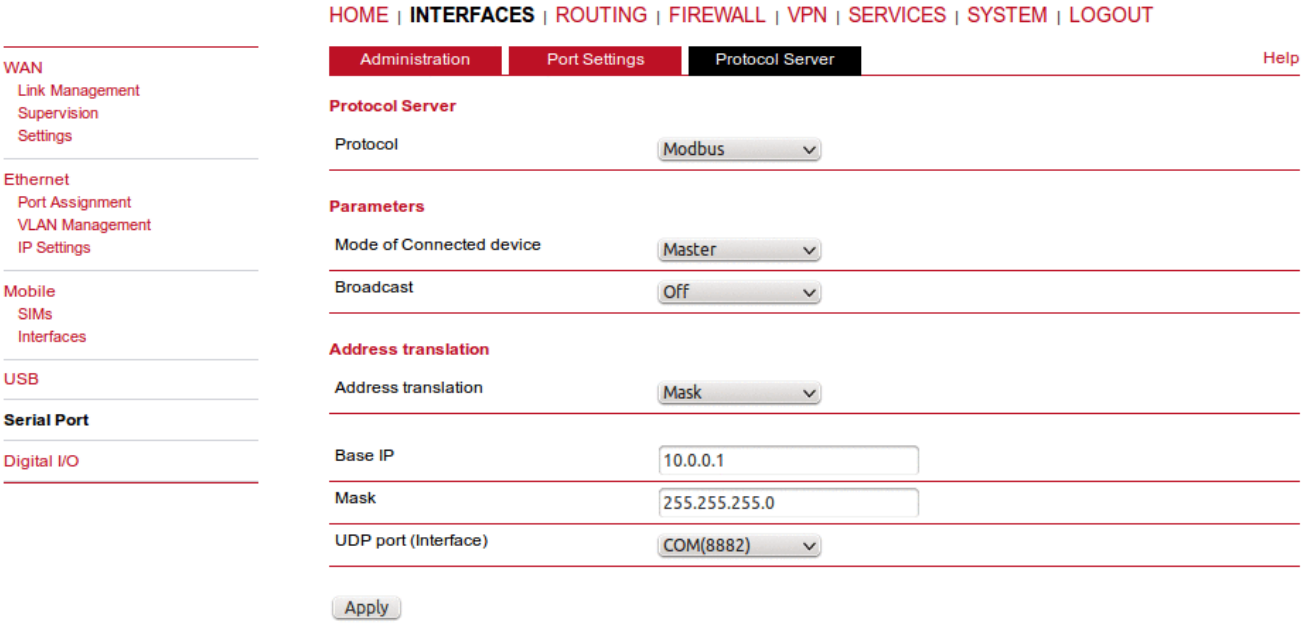
Protocol on IP port:	“Telnet” or “TCP raw”
Port:	The TCP port used by the application.
Timeout:	Endless or numbered (in seconds).
Allow remote control (RFC 2217)	Telnet with the RFC 2217 extension.
Show banner	The option for displaying the banner of the connected serial device.
Allow clients from	The option for limiting the access based on the host IP address.

Important

The UDP Device Server functionality has been moved into SDK only. The required script for this functionality can be provided on demand.

Protocol Server

The port settings configuration is the same as with the Device Server – the section called “Device Server”. Ignore the Server Configuration parameters, they do not have any effect. The protocol must be set in the Protocol Server menu.



Each SCADA protocol like Modbus, DNP3, IEC101, DF1 etc. has its unique message format, most importantly its unique way of addressing the remote units. The following text is valid for all M!DGE/MG102i/RipEX units (further in this the section called “Protocol Server” referred to as a "Unit") - the special properties for mobile GPRS/UMTS networks (e.g. limitation of broadcasting) are mentioned here. The basic task for the protocol server is to check whether a received frame is within the protocol format and is not corrupted. Most of the SCADA protocols are using some type of Error Detection Code (Checksum, CRC, LRC, BCC, etc.) for data integrity control, so each Unit calculates this code and checks it against the received one.

GPRS/UMTS mobile network operates in IP environment, so the basic task for the Protocol server is to convert SCADA serial packets to UDP datagrams. The Address translation settings are used to define the destination IP address and UDP port. Then these UDP datagrams are sent to the M!DGE/MG102i router, processed there and are forwarded as unicasts through the mobile network to their destination. When the gateway defined in the Routing table belongs to the Ethernet LAN, UDP datagrams are instead forwarded to the Ethernet interface. After reaching the gateway, the datagram is forwarded according to the Routing table.

When the UDP datagram reaches its final IP destination, it should be in a M!DGE/MG102i or RipEX router again. It is processed further according to its UDP port. It can be delivered to the Protocol server where where the datagram is decapsulated and the data received on the serial interface of the source unit are forwarded to COM. The UDP port can also be that of a Terminal server (RipEX) or any other special protocol daemon on Ethernet like Modbus TCP etc. The datagram is then processed according to the respective settings.

Received frames on COM are closed when the gap between bytes is longer than the Idle value. This parameter defines the maximum gap (in milliseconds) in the received data stream. If the gap exceeds this value, the link is considered idle, the received frame is closed and forwarded to the network.

The default Idle size differs based on the COM baud rate configuration. Remember that the default Idle sizes are set to the minimal possible values:

bps	**ms**
115200	120
57600	60
38400	30
19200	20
9600	10
4800	5
2400	5
1200	5
600	5
300	5

MRU (Maximum Reception Unit) – an incoming frame is closed at this size even if the stream of bytes continues. Consequently, a permanent data stream coming to COM results in a sequence of MRU-sized frames sent over the network. The default value is set to 1600 bytes.

Both values are configurable only in the configuration file located at /etc/config/factory-config.cfg as the following variables:

- *rrsp.2.Rrsp2Main_v1.0.COM_IDLE_SIZE=5*
- *rrsp.2.Rrsp2Main_v1.0.COM_MTU=1600*

Restart the rrsp2 daemon for changes to take effect (*# /etc/init.d/rrsp2 restart*).

Note

All timeouts in the parameters described below are derived from the time when the packet is sent into the COM driver, i.e. it includes the transfer time of the packet. Take this into account especially when there is a low Baud rate set in the COM settings.

Important

If configuring the Protocol server together with VPN tunnels, there are several extra steps which must be done. Please see the Application note, chapter 4.2 SCADA Protocols - public APN[1] for the details.

Common parameters

The parameters described in this section are typical of most protocols.
There is only a link to them in description of the respective Protocol.

Mode of Connected device
List box: Master, Slave
Default = Master
The typical SCADA application follows the Master–Slave scheme where the structure of the message is different for the Master and Slave SCADA units. Because of that, it is necessary to set which type of SCADA unit is connected to the Unit.

Important

For the SCADA Master, set Master, for the SCADA Slave, set Slave.

- **Master**
  TheSCADA Master always sends addressed messages to Slaves. Addressing is different for each SCADA protocol, so this is one of the main reasons why an individual Protocol server in each Unit for each SCADA protocol has to be used.
  - **Broadcast**
    List box: On, Off
    Default = Off
    Some Master SCADA units send broadcast messages to all Slave units. SCADA applications typically use a specific address for such messages. RipEX (Protocol utility) converts such messages into a customized IP broadcast and broadcasts it to all RipEX units resp. to all SCADA units within the network.

    Note

    Broadcasts in the GPRS/UMTS network are not possible, thus setting of broadcast functionality is not allowed with M!DGE/MG102i units.

    If **On**, the address for broadcast packets in the SCADA protocol has to be defined:
    - **Broadcast address format** - List box Hex, Dec - format in which the broadcast address is defined.
    - **Broadcast address** - address in the defined format (Hex, Dec)
  - **Address translation**
    List box: Table, Mask
    Default = Mask
    In a SCADA protocol, each SCADA unit has a unique address, a "Protocol address". In a GPRS/UMTS mobile network, each SCADA unit is represented by an IP address (typically that of the ETH interface) and a UDP port (that of the protocol daemon or the COM port server to which the SCADA device is connected via serial interface).
    A translation between the "Protocol address" and the IP address & UDP port pair has to be done. It can be done either via Table or Mask.

[1] http://www.racom.eu/eng/products/m/midge/app/SCADA_Serial_Protocols.html#SCADA_Protocols_public_APN

Hence, a SCADA message received from the serial interface is encapsulated into a UDP/IP datagram, where the destination IP address and the destination UDP port are defined according to the settings of the Address translation.

- **Mask**

  Translation using the Mask is simpler to set, however it has some limitations:
  − all IP addresses used have to be within the same network, which is defined by this Mask
  −the same UDP port is used for all the SCADA units, which results in the following:
  − SCADA devices on all sites have to be connected to the same interface
  − only one SCADA device can be connected to one COM port

  - **Base IP**
    Default = IP address of the ETH interface
    When creating the IP destination address of UDP datagram, in which the serial SCADA message received from COM is encapsulated, thi is created, this Base IP is taken as the basis and only the part defined by the Mask is replaced by the 'Protocol address'.
  - **Mask**
    Default = 255.255.255.0
    A part of the Base IP address defined by this Mask is replaced by the 'Protocol address'. The SCADA protocol address is typically 1 byte, so Mask 255.255.255.0 is most frequently used.
  - **UDP port (Interface)**
    List box: COM, Manual
    This UDP port is used as the destination UDP port in the UDP datagram in which the serial SCADA packet received from COM1 is encapsulated. The default UDP port for COM can be used or the UDP port can be set manually. If the destination IP address belongs to a Unit and the UDP port is not assigned to COM (COM1(2) or to a Terminal server in case of RipEX) or to any special daemon running in the destination address, the packet is discarded.

Note

M!DGE/MG102i use UDP port 8882 for its COM port.

- **Table**
  The Address translation is defined in a table. There are no limitations such as when the Mask translation is used. If there are more SCADA units on the RS485 (e.g. with RipEX COM2) their interface, their “Protocol addresses” should be translated to the same IP address and UDP port pair, where the multiple SCADA units are connected. There are 3 possibilities how to fill in the line in the table:
  − One "Protocol address" to one "IP address" (e.g.: 56 −−> 192.168.20.20)
  − Range of "Protocol addresses" to one "IP address" (e.g.: 56 – 62 ===> 192.168.20.20)
  − Range of "Protocol addresses" to range of "IP addresses" (e.g.: 56 – 62 ===> 192.168.20.20 – 26). One option is to write only the start IP and a dash, the system will add the end address itself.
  - **Protocol address**
    This is the address which is used by the SCADA protocol. It may be set either in Hexa-decimal or Decimal format according to the List box value.
    Protocol address length can be 1 byte, but for the DNP3 and UNI protocols support 2 bytes addresses.
  - **IP**
    The IP address to which Protocol address will be translated. This IP address is used as the destination IP address in the UDP datagram in which serial SCADA packet received from COM is encapsulated.

- **UDP port (Interface)**
  This is the UDP port number which is used as the destination UDP port in the UDP datagram in which the serial SCADA message, received from COM, is encapsulated.
- **Note**
  You may add a note to each address up to 16 characters long for your convenience. (E.g. “Remote unit #1”).
- **Active**
  You may tick/un-tick each translation line in order to make it active/not active.
- **Modify**
  Edit, Delete Add buttons allow to edit or to add or to delete a line. The lines can be sorted using up and down arrows.

- **Slave**
  The SCADA Slave typically only responds to Master requests, however in some SCADA protocols it can communicate spontaneously.
  Messages from the serial interface are processed in a similar way as the Master site, i.e. they are encapsulated in UDP datagrams, processed by the router inside the M!DGE/MG102i unit and forwarded to the respective interface, typically to the mobile network.
  - **Broadcast accept**
    List box: On, Off
    Default = Off
    If **On**, broadcast messages from the Master SCADA device to all Slave units are accepted and sent to connected Slave SCADA unit.

Important

Broadcasting is not supported with mobile networks.

PROTOCOLS IMPLEMENTED:

None

All received frames from the COM port as well as from the network are discarded.

Async link

The async link creates asynchronous link between two COM ports on different Units. Received frames from COM are sent without any processing transparently to the mobile network to set the IP destination and UDP port. Received frames from the mobile network are sent to the respective COM according to the UDP port setting.

- **Parameters**
  - **Destination IP**
    This is the IP address of the destination Unit.
  - **UDP port (Interface)**
    This is the UDP port number which is used as the destination UDP port in the UDP datagram in which the packet received from COM is encapsulated.

C24

C24 is a serial polling-type communication protocol used in Master–Slave applications.

Multiple C24 Masters can be used within one network and one Slave can be polled by more than one Master.

Underlined parameters are described in *Common parameters*.

Mode of Connected device

Master

Address translation

Table

Mask

Slave

- **Protocol frames**
  List box: 1C, 2C, 3C, 4C
  Default = 1C
  One of the possible C24 Protocol frames can be selected.

- **Frames format**
  List box: Format1, Format2, Format3, Format4, Format5
  Default = Format1
  One of the possible C24 Frames formats can be selected. According to the C24 protocol specification, it is possible to set Frames formats 1–4 for Protocol frames 1C–3C and formats 1–5 for 4C.

Important

The Unit accepts only the set Protocol frames and Frames format combination. All other combinations frames are discarded by the Unit and not passed to the application.

- **Local ACK**
  List box: Off, On
  Default = Off
  Available for Protocol frame 1C only. When **On**, ACK on COM is send locally from this unit, not over the mobile network.

Cactus

Cactus is a serial polling-type communication protocol used in Master–Slave applications.
Multiple Cactus Masters can be used within one network and one Slave can be polled by more than one Master.

Underlined parameters are described in Common parameters.

Mode of Connected device

Master

Broadcast

Note: There is no the possibility to set Broadcast address, since Cactus broadcast messages always have the address 0x00. Hence when the Broadcast is On, packets with this destination are handled as broadcasts. Broadcasting is not supported with mobile networks.

Address translation

Table

Mask

Slave

Broadcast accept

- **Max gap timeout [ms]**
  Default = 30
  The longest time gap for which a frame can be interrupted and still received successfully as one frame. It should not be set below 10ms, while 15–40 ms should be OK for a typical Cactus protocol device.

Comli

Comli is a serial polling-type communication protocol used by Master–Slave applications.
More Comli Masters can be used within one network and one Slave can be polled by more Masters.
Broadcasts packets are not used, so the configuration is using only some parameters described in *Common parameters*.

Mode of Connected device

Master

Address translation

Table

Mask

Slave

DF1

Only the full-duplex mode of DF1 is supported. Each frame in the Allen-Bradley DF1 protocol contains the source and destination addresses in its header, so there is no difference between Master and Slave in the full-duplex mode in terms of Unit configuration.

- **Block control mode**
  List box: BCC, CRC
  Default = BCC
  According to the DF1 specification, either BCC or CRC for Block control mode (data integrity) can be used.
- **Broadcast**
  According to the DF1 specification, packets for the destination address 0xFF are considered broadcasts. Broadcasts are not supported with the mobile network.

Address translation

Table

Mask

- **Advanced parameters**
  - **ACK Locally**
    List box: Off, On
    Default = On
    If "**On**", ACK frames (0x1006) are not transferred over-the-air.

When the Unit receives a data frame from the connected device, it generates the ACK frame (0x1006) locally. When the Unit receives the data frame from the mobile network, it sends the frame to the connected device and waits for the ACK. If the ACK is not received within 1 sec. timeout, Unit sends ENQ (0x1005). ENQ and ACK are not generated for broadcast packets.

DNP3

Each frame in the DNP3 protocol contains the source and destination addresses in its header, so there is no difference between Master and Slave in terms of the M!DGE/MG102i configuration. The DNP3 allows both Master–Slave polling as well as spontaneous communication from remote units.

- **Broadcast -** Note: There is not the option to set the Broadcast address, since DNP3 broadcast messages always have addresses in the range 0xFFFD – 0xFFFF. Broadcasting is not supported by mobile networks, thus it is not possible to set the broadcast to On..

Address translation

Table

Mask

IEC 870-5-101

IEC 870-5-101 is a serial polling-type communication protocol used by Master–Slave application.
More IEC 870-5-101 Masters can be used within one network and one Slave can be polled by more Masters.
IEC 870-5-101 protocol configuration is using all parameters described in *Common parameters*.

Mode of Connected device

Master

Broadcast - only On, Off. Protocol broadcast address is not configurable, it is defined by Address mode in Advance parameter (default 0xFF), but broadcasting is not allowed within mobile networks.

Address translation

Table

Mask

Slave

Broadcast accept

- **Advanced parameters**
  - **Address mode**
    Even if IEC 870-5-101 is the standard, there are some users who have customized this standard according to their needs. If addressed byte has been moved, M!DGE/MG102i/RipEX has to read it at the correct frame position.
    - **IEC101**
      Address byte location according to IEC 870-5-101 standard.
      Broadcast from Master station is generated when address byte is 0xFF.
    - **2B ADDR**
      Two byte address (IEC 870-5-101 standard is 1 byte). The frame is 1 byte longer than the standard one. There is the Intel sequence of bytes: low byte, high byte. Mask Address translation has to be used, because Table one is limited to just one byte address length.

The Master station broadcast is generated when the low address byte is 0xFF and high address byte is also 0xFF.

- **TELEGYR**
  The Control byte in the standard IEC packet is omitted. The frame is 1 byte shorter than a standard one. This is typically used in the Telegyr 805/809 protocol.
  Broadcast from Master station broadcast is generated when the address byte is 0x00.
- **SINAUT**
  The sequence of Address byte and Control byte in the frame is swapped-over.
  Master station broadcast is generated when the address byte is 0x00.

ITT Flygt

ITT Flygt is a serial polling-type communication protocol used in Master–Slave applications.

ITT Flygt protocol configuration uses all parameters described in *Common parameters*.

Mode of Connected device

Master

Broadcast

Note: There is no possibility to set the Broadcast address, since ITT Flygt broadcast messages always have the address 0xFFFF. Hence when the Broadcast is **On**, packets with this destination are handled as broadcasts. Broadcasting is not available with mobile GPRS/UMTS networks.

- **First Slave Address**
  Default = 1
  Slave addresses are not defined in the ITT Flygt protocol. However Slave addresses have to be defined in the Unit network. This is the First Slave address in decimal format.
- **Number of Slaves**
  Default = 1
  Since the ITT Flygt protocol Master (centre) polls the Slaves (remotes) one by one without any addressing, the number of Slaves has to be defined.

Address translation

Table

Mask

Slave

Broadcast accept

- **Wait timeout [ms]**
  Default = 5000
  An ITT Flygt Slave sometimes sends the WAIT COMMAND (0x13) to its Master. The Unit does not accept the next WAIT COMMAND (discards it), till the Wait timeout expires. The Recommended value is in the 1–10 seconds range.

Modbus

Modbus RTU is a serial polling-type communication protocol used by Master–Slave application.

More Modbus Masters can be used within one network and one Slave can be polled by more Masters. Modbus protocol configuration uses all parameters described in *Common parameters*.

Mode of Connected device
- *Master*
  - *Broadcast*
  - *Address translation*
    - *Table*
    - *Mask*
- *Slave*
  - *Broadcast accept*

Profibus

RipEX supports Profibus DP (Process Field Bus, Decentralized Periphery) the widest-spread version of Profibus. The Profibus DP is supported even by M!DGE/MG102i, but it will work satisfactorily only with mobile networks with very short transport delays, like LTE or UMTS. The Profibus protocol configuration uses all parameters described in Common parameters.

Mode of Connected device
- *Master*
  - *Broadcast*
  - *Address translation*
    - *Table*
    - *Mask*
- *Slave*
  - *Broadcast accept*

RP570

RP570 is a serial polling-type communication protocol used in Master–Slave applications.

Multiple RP570 Masters can be used within one network and one Slave can be polled by more than one Master.

Underlined parameters are described in *Common parameters*.

Mode of Connected device
- *Master*

- **Local simulation RB**
  List box: Off, On
  Default = Off
  The RP570 protocol Master very often transmits the RB packets (hold packets) solely to check whether Slaves are connected. In order to minimize the mobile network payload, the Unit can be configured to respond to these packets locally and not to transmit them to the Slaves over the mobile network.

If **On**, the Unit responds to RB packets received from the RP 570 master locally over the COM interface. However from time to time (RB period) the RB packets are transferred over the network in order to check whether the respective Slave is still on. When the RB response from the Slave to this RB packet is not received over the mobile network within the set RB timeout, i.e. the respective Slave is out of order, the central Unit stops local answering to RB packets from the master for the respective Slave.

- **RB Net period [s]**
  Default = 10
  The M!DGE/MG102i/RipEX responds to the RB packets locally and in the set RB period the RB packets are transferred over the network.

- **RB Net timeout [s]**
  Default = 10 (maximum=8190)
  Whenever an RB packet is sent over the network, the set RB Net timeout starts. When the RB response from the remote unit (Slave) is not received within the timeout, i.e. the respective Slave is out of order, the central Unit stops the local answering to RB packets from the master for the respective Slave.

Address translation

Table

Mask

Slave

Slave

- **Local simulation RB**
  List box: Off, On
  Default = Off
  The RP570 Slave expects to receive RB packets from the Master. When the Local simulation RB on the Master is On, the RB packets are transferred over the mobile network only in the RB Net period (see the Master settings). The Local simulation RB has to be set the same (On or Off) on all sites in the network, i.e. on the master as well as all Slaves.

  If **On**, the Unit generates RB packets locally and transmits them over the COM interface in the RB Request period and expects the RB response for each RB packet from the RP570 Slave within the RB Response timeout. When the Unit does not receive the response(s) from the RP570 Slave, the Unit does not respond to the RB packet from the Master, which it receives over the mobile networks.

- **RB Request period [ms]**
  Default = 200 (maximum=8190)
  M!DGE/MG102i/RipEX sends locally RB packets to the connected RTU in the set period.

- **RB Response timeout [ms]**
  Default = 500 (maximum=8190)
  The Unit expects a response to the RB packet within the set timeout. If it is not received, the Unit does not respond to RB packets from the Master received over the mobile network.

- **RTU address (Hex)**
  Default = 01

Active only when the Local simulation RB is On. The connected RTU's address is supposed to be filled in. This address (0x00-0xFF) is used in the RB packets generated locally in the M!DGE/MG102i/RipEX and transmitted over the COM.

Siemens 3964(R)

The 3964 protocol is utilized by the Siemens Company as a Point-to-Point connection between two controllers. Meanwhile it has become an industry standard that can be found on many devices as a universal communications interface. 3964R is the same as 3964, in addition it only uses BCC (Block Check Character). 3964(R) handle only the link layer (L2 in OSI model), hence Unit uses a similar way to read "SCADA address" as in UNI protocol.

There is a handshake STX(0x02) – DLE(Ox10) at the start of communication and DLE+ETX – DLE at the end. This handshake is performed by RipEX locally, it is not transferred over the RipEX network.

Communication goes as follows:
LocalRTU→STX→LocalRipex
LocalRipex→DLE→LocalRTU
LocalRTU→DATA+DLE+ETX+BCC→LocalRipex
LocalRipex→DATA→RemoteRipex*
LocalRipex→DLE→LocalRTU
RemoteRipex→STX→RemoteRTU
RemoteRTU→DLE→RemoteRipex
RemoteRipex→DATA+DLE+ETX+BCC→RemoteRTU
RemoteRTU→DLE→RemoteRipex

* only this packet is transferred over the RipEX network, all the other ones are handled locally.

Underlined parameters are described in *Common parameters*.

Mode of Connected device

Master

- **Address mode**
  List box: Binary (1 B), Binary (2B LSB first). Binary (2B MSB first).
  Default = Binary (1 B)
  M!DGE/MG102i/RipEX reads the Protocol address in the format and length set (in bytes).
- **Address position**
  Specify the sequence number of the byte, where the Protocol address starts.

  Note 1: 3964(R) protocol uses an escape sequence (control sequence) for DLE (0x10), i.e. when 0x10 is in user data, 0x1010 is sent instead. When the address position is calculated, the bytes added by the escape sequence algorithm are not taken into account.

  Note 2: The first byte in the packet has the sequence number 1, not 0.

Broadcast

Address translation

Table

Mask

Slave

Broadcast accept

- **DLE timeout [ms]**
  Default = 1000 (min. 300, max. 8190)

  M!DGE/MG102i/RipEX expects a response (DLE) from the connected device (RTU) within the set timeout. If it is not received, the Unit repeats the frame according to the “Retries” setting.

- **Retries [No]**
  Default = 3 (min. 0, max. 7)

  When DLE timeout is „On“, and the DLE packet is not received from the connected device (RTU) within the set DLE timeout, the Unit retransmits the frame. The number of possible retries is specified.

- **Priority**
  List box: Low, High
  Default = Low

  When the equipment sends STX and receives STX instead of DLE, there is a collision, both devices want to start communication. In such a case, one unit has to have priority. If the Priority is High, the Unit waits for DLE. When it is Low, the Unit send DLE.

  Note: Obviously, two devices which are communicating together must be set so that one has High priority and the other has Low.

- **BCC**
  List box: On, Off
  Default = On

  BCC (Block Check Character) is a control byte used for data integrity control, it makes the reliability higher. BCC is used by 3964R, 3964 does not use it.

  The unit checks (calculates itself) this byte while receiving a packet on COM. Unit transmits DLE (accepts the frame) only when the check result is OK. The BCC byte is not transferred over the network, it is calculated locally in the end Unit and appended to the received data.

UNI

UNI is the "Universal" protocol utility designed by RACOM. It is supposed to be used when the application protocol is not in the Unit list. The key condition is that messages generated by the Master application device always contain the respective Slave address and that address (or its relevant part) position, relative to the beginning of the message (packet, frame), is always the same (Address position).

Generally two communication modes are typical for the UNI protocol: In the first one, communication always has to be initiated by the Master and only one response to a request is supported; in the second mode, Master-Master communication or combination of UNI protocol with ASYNC LINK protocol and spontaneous packet generation on remote sites are possible.

The UNI protocol is fully transparent, i.e. all messages are transported and delivered in full, without any modifications.

Underlined parameters are described in *Common parameters*.

Mode of Connected device

Master

- **Address mode**
  List box: Binary (1 B), ASCII (2 B), Binary (2B LSB first). Binary (2B MSB first).
  Default = Binary (1 B)
  M!DGE/MG102i/RipEX reads the Protocol address in the format and length set (in bytes).

  The ASCII 2-byte format is read as 2-character hexadecimal representation of one-byte value. E.g. ASCII characters AB are read as 0xAB hex (10101011 binary, 171 decimal) value.
- **Address position**
  Specify the sequence number of the byte, where the Protocol address starts. Note that the first byte in the packet has the sequence number 1, not 0.
- **Address mask (Hex)**
  When the Address mode is Binary 2 bytes, a 16-bit value is read from the SCADA protocol message according to the Address mode setting (either the MSB or the LSB first), The resulting value is then bit-masked by the Address mask and used as the input value for SCADA to IP address translation (e.g. via a table). The default value of the Address mask is 0xFFFF, hence the full 16-bit value is used by default.

  Example:
  The Address mode is set to Binary (2B LSB first), the Address mask is set to 7FF0 and the Address position is set to 2. The SCADA message starts with bytes (in hex) 02 DA 92 C3 .. The 2-byte address is read as 0x92DA (note the LSB came first in the message), Then 0x7FF0 mask is applied and the resulting value 0x12D0 (0x92DA & 0x7FF0) is used as the input for the translation.
- **Poll response control**
  List box: On, Off
  Default = On

  On – The Master accepts only one response per request and it must come from the the specific remote to which the request was sent. All other packets are discarded. This applies to the Master–Slave communication scheme.

  Note: It may happen, that a response from a Slave (No.1) is delivered after the respective timeout expired and the Master generates the request for the next Slave (No.2) in the meantime. In such a case the delayed response from No.1 would have been considered as the response from No.2. When Poll response control is On, the delayed response from the Slave No.1 is discarded and the Master stays ready for the response from No.2.

  Off – The Master does not check packets incoming from the mobile network - all packets are passed to the application. That allows e.g. spontaneous packets to be generated at remote sites. This mode is

suitable for the Master–Master communication scheme or a combination of the UNI and ASYNC LINK protocols.

Broadcast

Address translation

Table

Mask

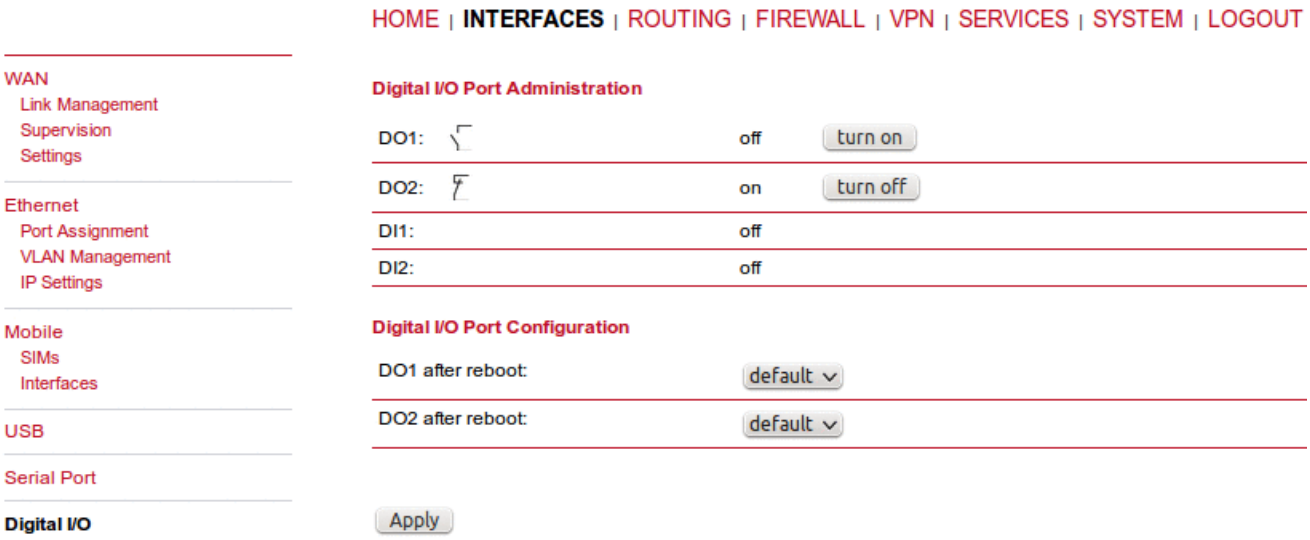
Slave

Broadcast accept

7.2.6. Digital I/O

The Digital I/O page displays the current status of the I/O ports and can be used to turn output ports on or off.

You can apply the following settings:



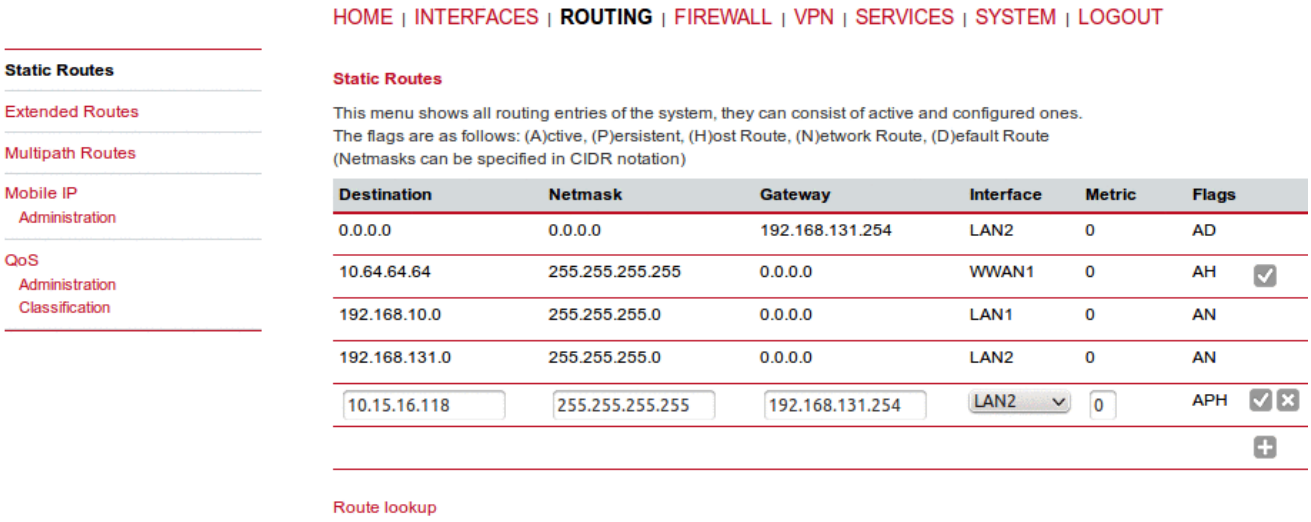
Besides on and off you may keep the status after reboot at default which corresponds to the default state as the hardware will be initialized at power-up.

The digital inputs and outputs can also be monitored and controlled by SDK scripts.

7.3. ROUTING

7.3.1. Static Routes

This menu shows all routing entries of the system, which can consist of active and configured ones. (Netmasks can be specified in CIDR notation, e.g. **24** expands to `255.255.255.0`).



Destination: Destination network or host provided by IP addresses in dotted decimal.

Netmask: Subnet mask which forms, in combination with the destination, the network to be addressed. A single host can be specified by a netmask of `255.255.255.255`, a default route corresponds to `0.0.0.0`.

Gateway: The next hop which operates as gateway for this network (can be omitted on peer-to-peer links).

Interface: Network interface on which a packet will be transmitted in order to reach the gateway or network behind.

Metric: The routing metric of the interface (default 0). The routing metric is used by routing protocols, higher metrics have the effect of making a route less favourable; metrics are counted as additional costs to the destination network.

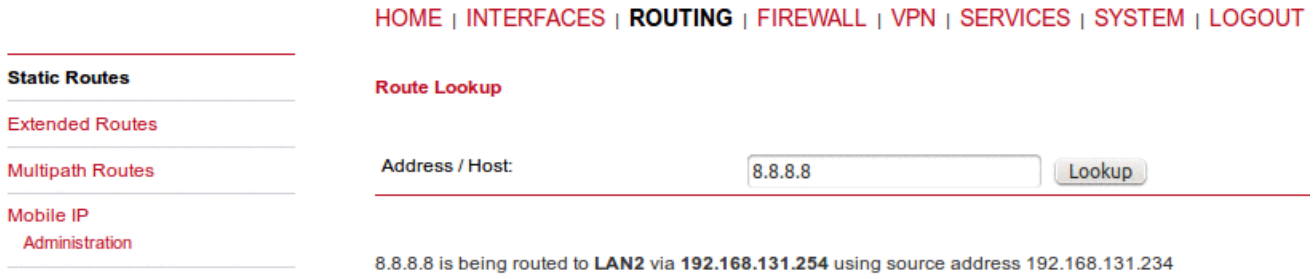
Flags: (A)ctive, (P)ersistent, (H)ost Route, (N)etwork Route, (D)efault Route

The flags obtain the following meanings:

Active	The route is considered active, it might be inactive if the interface for this route is not yet up
Persistent	The route is persistent, which means it is a configured route, otherwise it corresponds to an interface route
Host	The route is a host route, typically the netmask is set to 255.255.255.255.
Network	The route is a network route, consisting of an address and netmask which forms the subnet to be addressed

Default Route	The route is a default route, address and netmask are set to 0.0.0.0, thus matching any packet

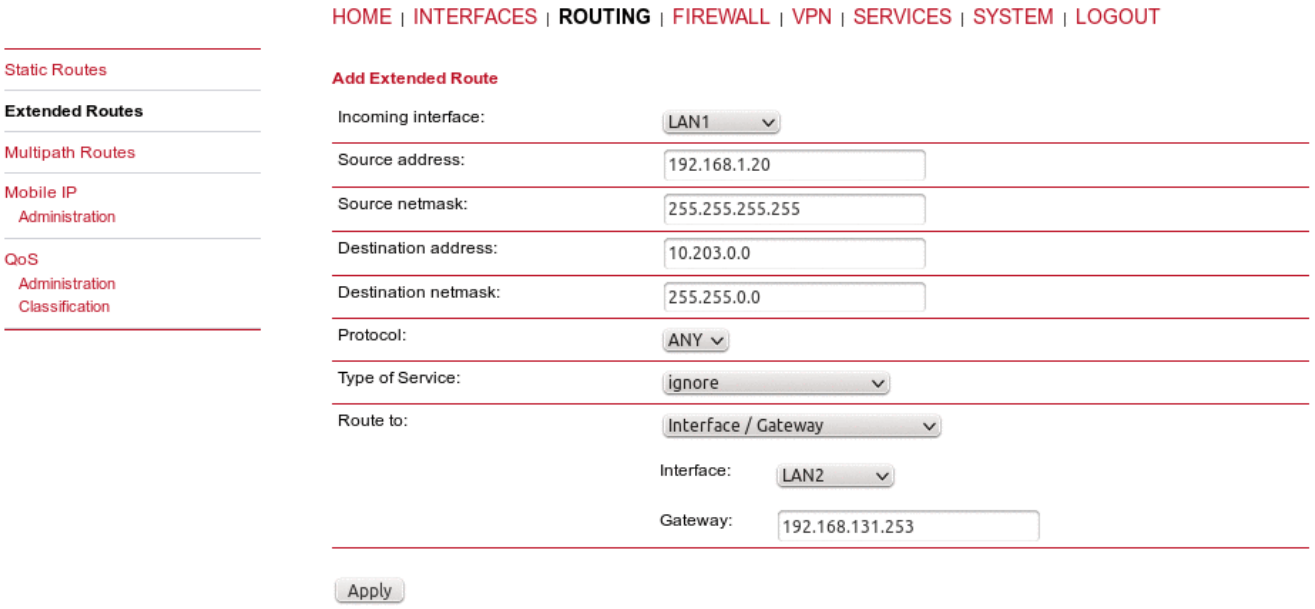
You can check the corresponding routing via the "Route lookup" functionality. Just fill in the desired IP address and click on the "Lookup" button. The detailed information about the chosen route will be displayed.



7.3.2. Extended Routes

Extended routes can be used to perform policy-based routing, they generally precede static routes.

Extended routes can be made up not only of a destination address/netmask but also a source address/netmask, incoming interface and the type of service (TOS) of packets.

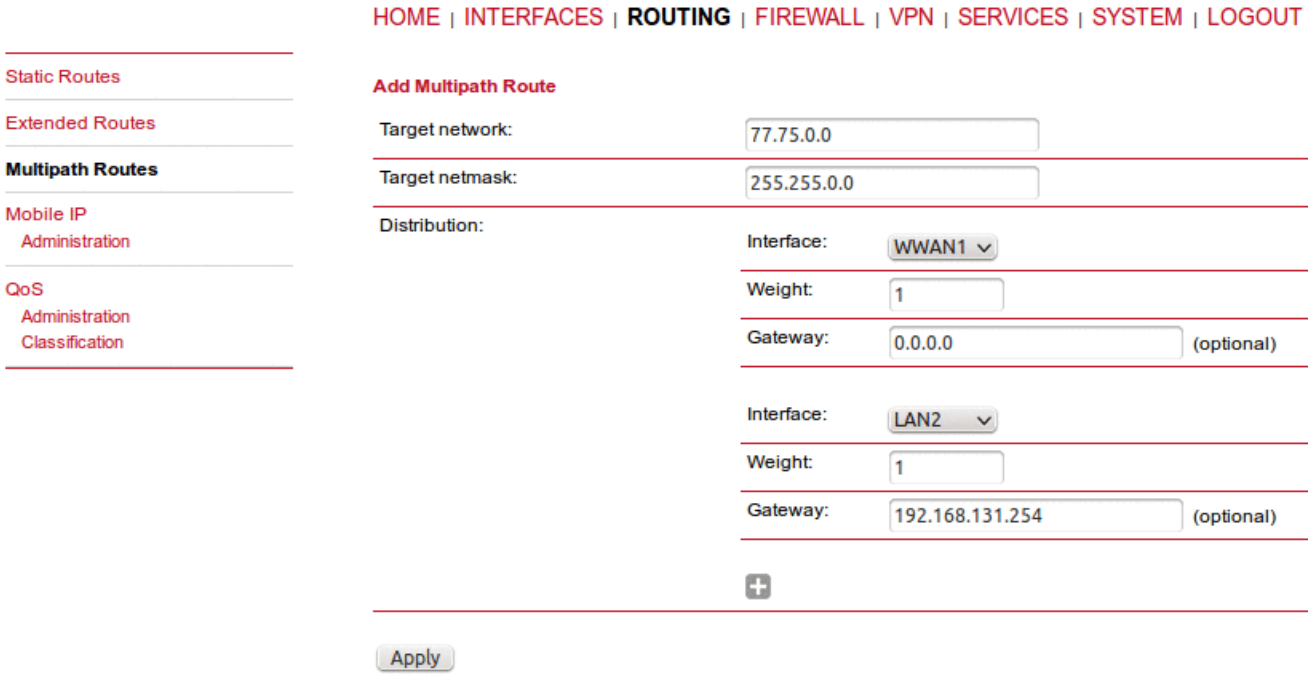


Incoming interface	The interface on which the packet enters the system
Source address	The packet source address
Source netmask	The packet source netmask
Destination address	The packet destination address
Destination netmask	The packet destination netmask
Protocol	Protocol used (ANY, UDP or TCP)
Type of service	The TOS value within the packet header

Route to	Specifies the target interface or gateway to where the packet should get routed to.
Type of Service	The ToS value within the packet header (possible values are ignore, normal-service (0), minimize-cost (2), maximize-reliability (4), maximize-throughput (8), minimize-delay (16))

7.3.3. Multipath Routes

Multipath routes perform weighted IP-session distribution for particular subnets across multiple interfaces.



At least two interfaces must be defined to establish the Multipath routing. Additional interfaces can be added by pressing the "plus" sign.

Target network/netmask	The target network for which the Multipath routing will be applied
Interface	The interface for the selected path
Weight	Interface weight in relation to the others (e.g. values 4 and 1 for two paths will result in 80 and 20 % of distribution)
Nexthop	Nexthop address to be used as a default gateway for the selected interface

7.3.4. Mobile IP

Mobile IP (MIP) can be used to enable a seamless switch between different WAN technologies.

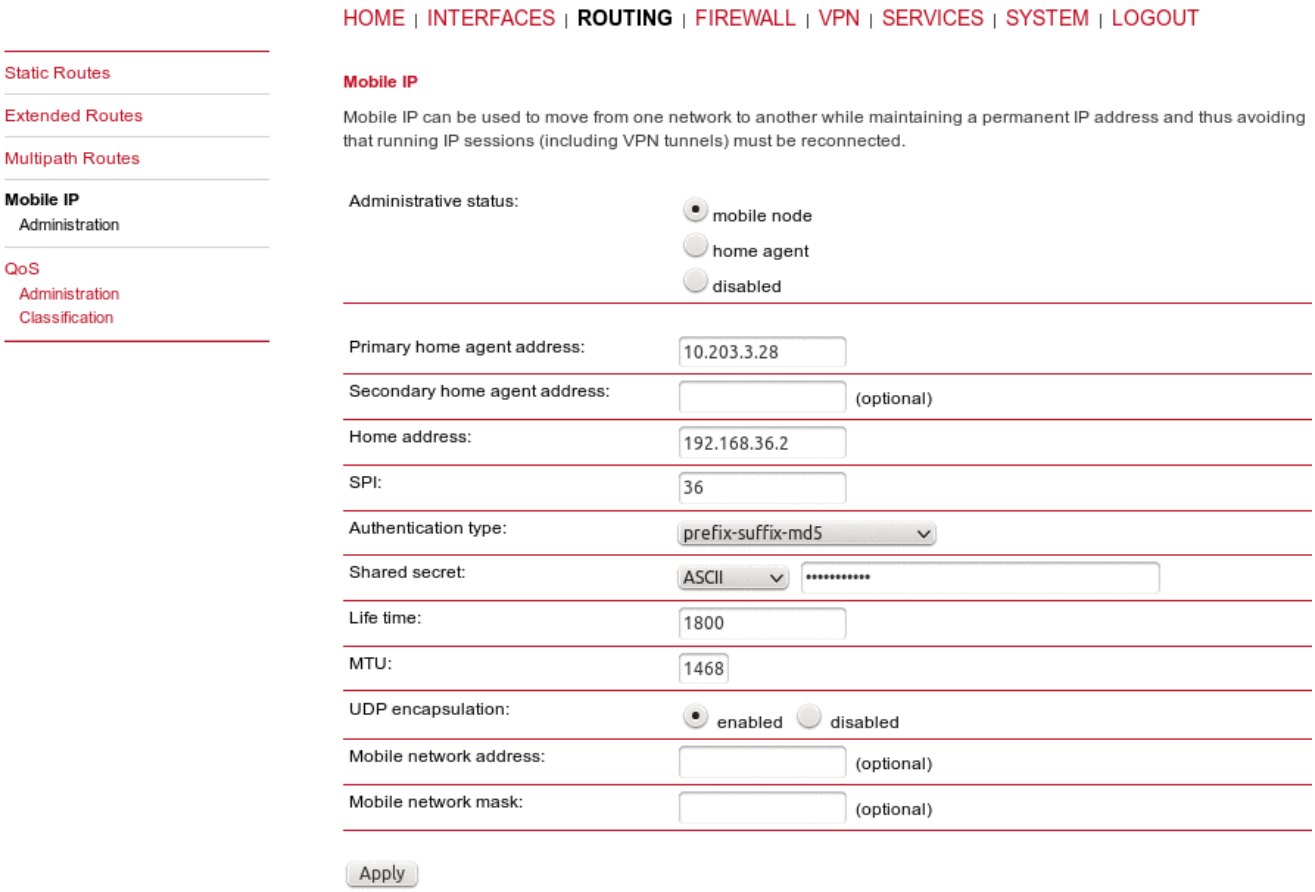
Note

A valid license key is required for running Mobile IP.

It boasts with very small outages during switchover while keeping all IP sessions alive which is being accomplished by communicating with the static public IP address of a home agent which will encapsulate

the packets and send them further to the router. Switching works by telling the home agent that the hotlink address has changed, the agent will then re-route (that means encapsulate the packets with the new target address) the packets transparently down to the box.

Our implementation supports RFC 3344, 5177, 3024 and 3519 and interoperability with Cisco has been verified. However, M!DGE/MG102i routers can run as node and home agent which makes them able to replace expensive kits in the backbone for smaller scenarios.



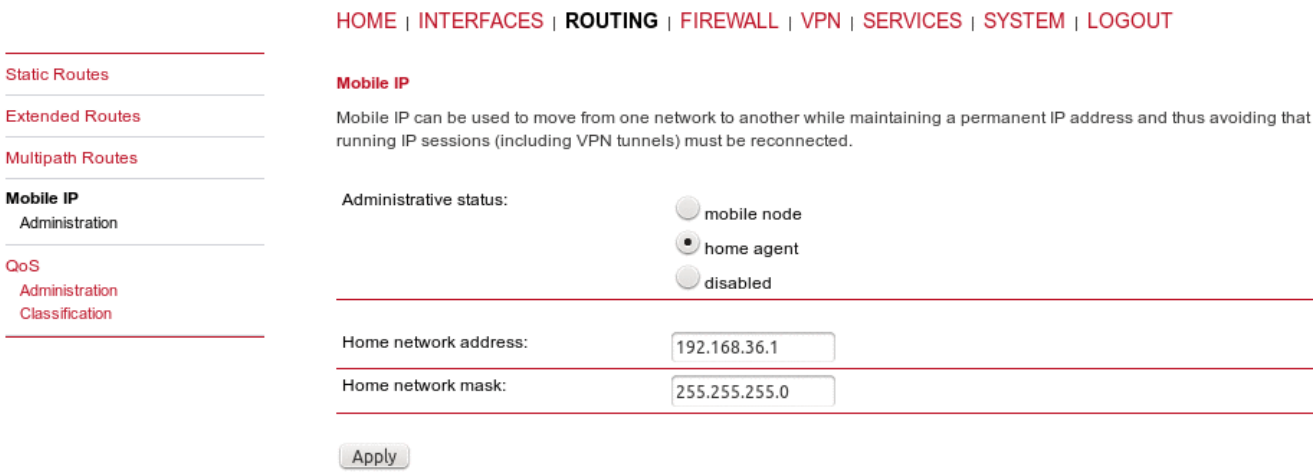
If MIP is run as the Mobile node, the following settings can be configured:

Primary home agent address:	The address of the primary home agent
Secondary home agent address:	The address of the secondary (fallback) home agent
Home address:	The permanent home address of the node which can be used to address the box
SPI:	The Security Parameter Index (SPI) identifying the security context between a pair of nodes (represented in 8 chars hex)
Authentication type:	The used authentication, can be prefix-suffix-md5 or hmac-md5
Shared secret:	The shared secret used for authentication, can be a 128-bit hex or ASCII string
Life time:	The lifetime of security associations in seconds
MTU:	Maximum transmission unit in bytes

UDP encapsulation: Specifies whether UDP encapsulation shall be used

Mobile network address: Optionally specifies a subnet which should be routed to the box

Mobile network mask: The netmask for the optional routed network



If MIP is run as home agent, you will have to set up a home address and netmask first and configure various nodes afterwards which are made up of the following settings:

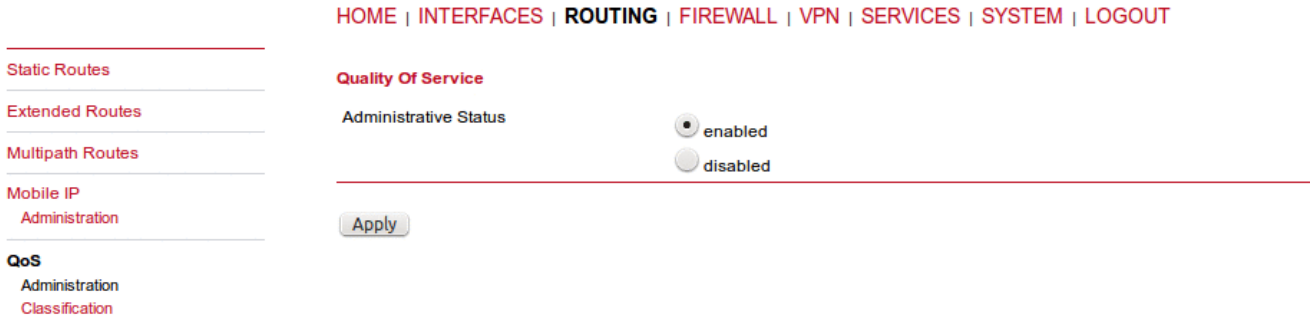
SPI The home address of the network

Authentication type The mask for the home network.

Shared secret The shared secret used for the mobile node authentication at the home agent. This can be either a 128-bit hexadecimal value or a random length ASCII string.

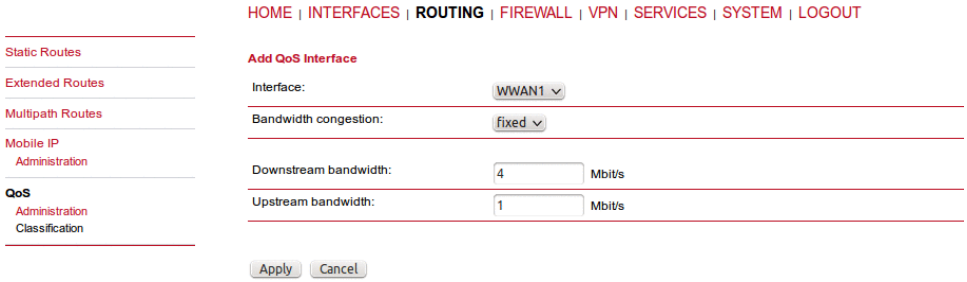
7.3.5. Quality of Service (QoS)

M!DGE/MG102i routers are able to prioritize and shape certain kinds of IP traffic. This is currently limited on egress, which means that only outgoing traffic can be stipulated. The current QoS implementation uses Stochastic Fairness Queueing (SFQ) classes in combination with Hierarchy Token Bucket (HTB) queuing disciplines. In case of demands for other classes or qdiscs, please contact our support team in order to evaluate the best approach for your application.



QoS Administration — The administration page can be used to enable and disable QoS.

QoS Classification — The classification section can be used to define the WAN interfaces on which QoS should be active.



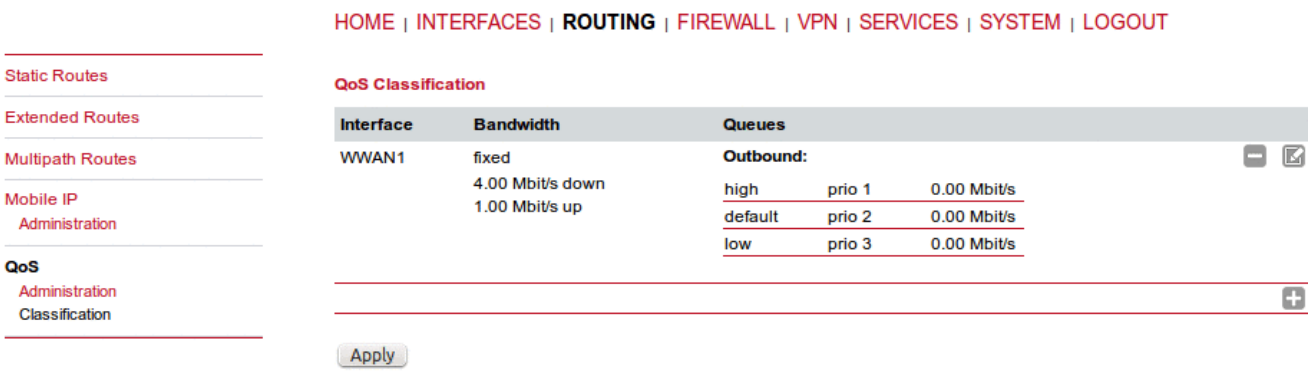
Interface: The WAN interface on which QoS should be active.

Bandwidth congestion: The bandwidth congestion method. In case of the auto option, the system will try to apply limits in a best-effort way. However, it is suggested to set fixed bandwidth limits as they also offer a way of tuning the QoS behaviour.

Downstream bandwidth: The available bandwidth for incoming traffic.

Upstream bandwidth: The available bandwidth for outgoing traffic.

When defining limits, you should consider bandwidth limits which are at least possible as most shaping and queues algorithms will not work correctly if the specified limits cannot be achieved. In particular, any WWAN interfaces operating in a mobile environment are suffering variable bandwidths, thus rather lower values should be used.

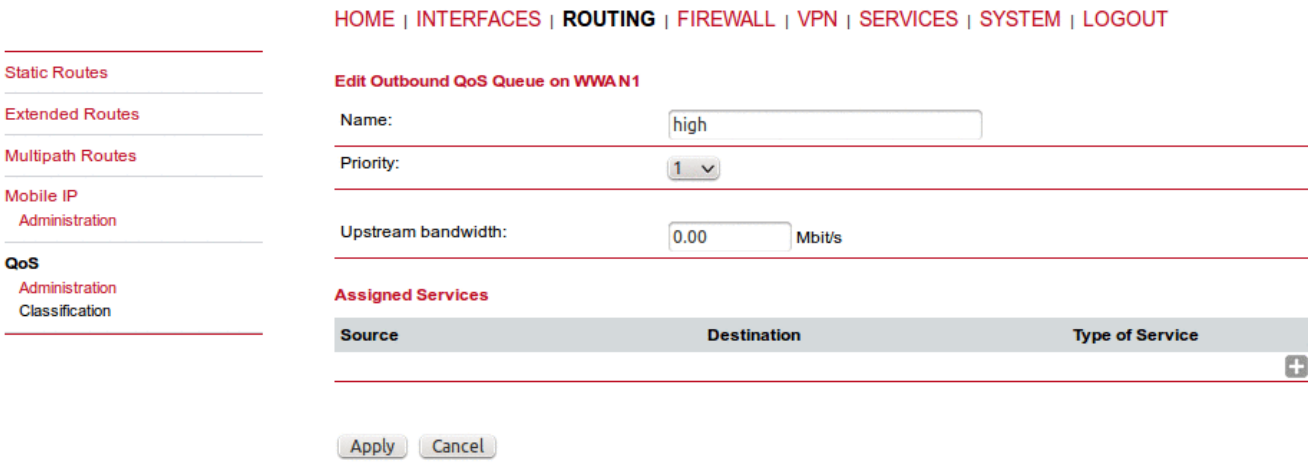


In case an interface has been activated, the system will automatically create the following queues:

high: A high priority queue which may hold any latency-critical services (such as VoIP).

default: A default queue which will handle all other services.

low: A low priority queue which may hold less-critical services for which shaping is intended.

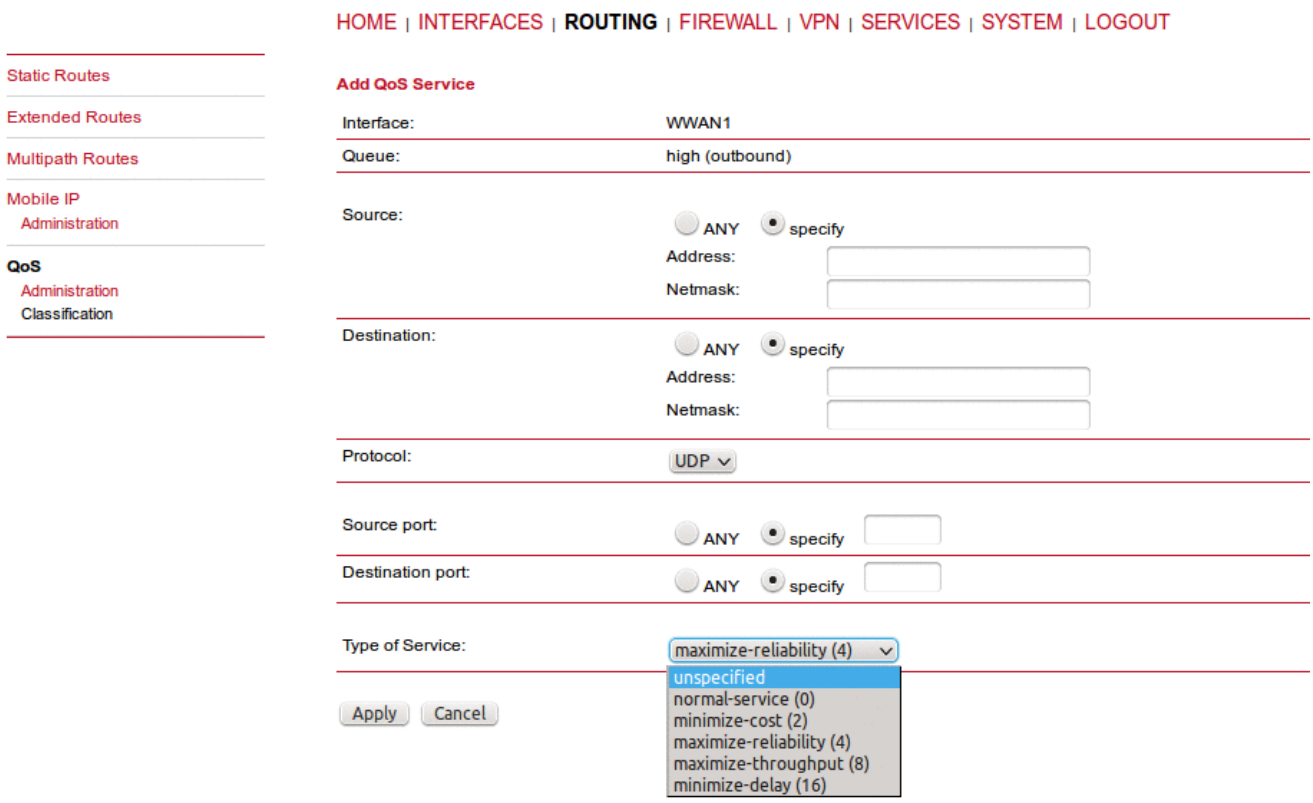


Each queue can be configured as follows:

Name: The name of the QoS queue.

Priority: A numerical priority for the queue, lower values indicate higher priorities.

Bandwidth: The maximum possible bandwidth for this queue.



You can now configure and assign any services to each queue. The following parameters apply:

Interface:	The QoS interface of the queue
Queue:	The QoS queue to which this service shall be assigned
Source:	Specifies a network address and netmask used to match the source address of packets
Destination:	Specifies a network address and netmask used to match the destination (target) address of packets
Protocol:	Specifies the protocol for packets to be matched
Type of Service:	Specifies the ToS/DiffServ for packets to be matched

7.4. FIREWALL

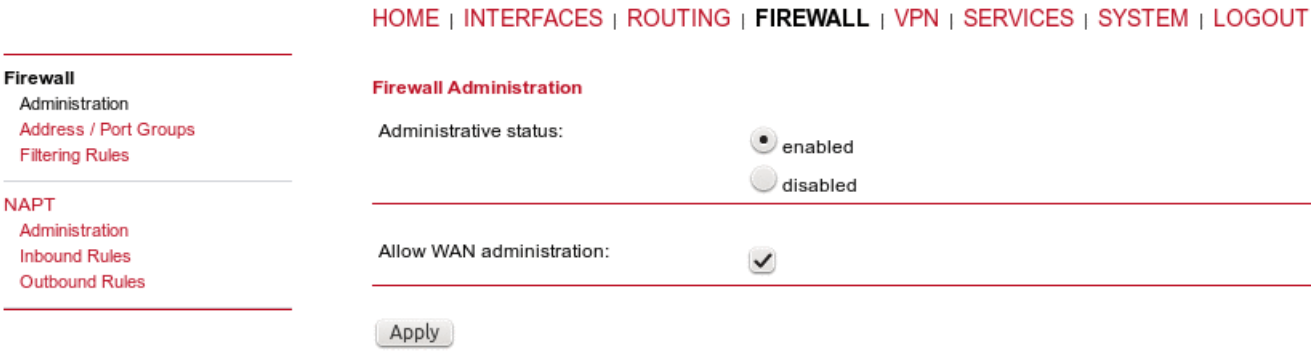
This router uses Linux's netfilter/iptables firewall framework (see http://www.netfilter.org for more information). It is set up of a range of rules which control each packet's permission to pass the router. Packets, not matching any of the rules, are allowed by default.

7.4.1. Firewall

Administration

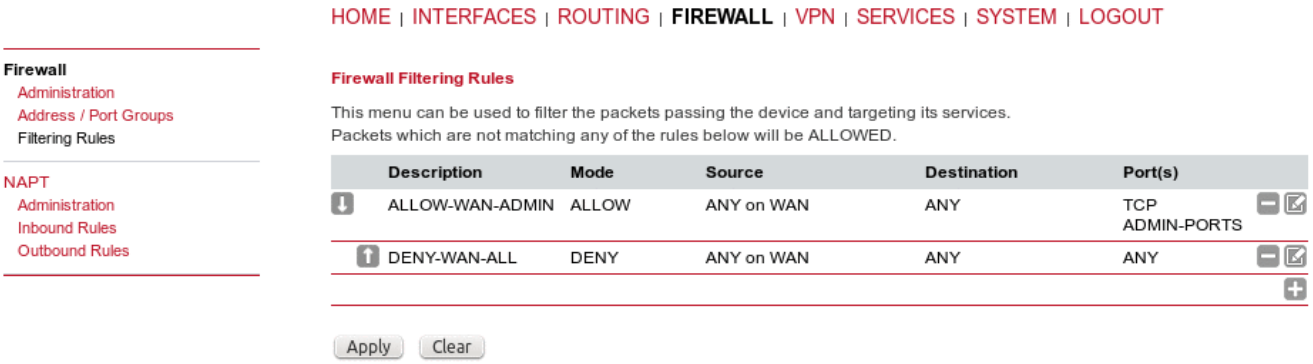
The administration page can be used to enable and disable firewalling. When turning it on, a shortcut can be used to generate a predefined set of rules which allow administration (over HTTP, HTTPS, SSH or TELNET) by default but block any other packets coming from the WAN interface. Please note that

the specified rules are processed by order, that means, traversing the list from top to bottom until a matching rule is found. If there is no matching rule found, the packet is allowed.



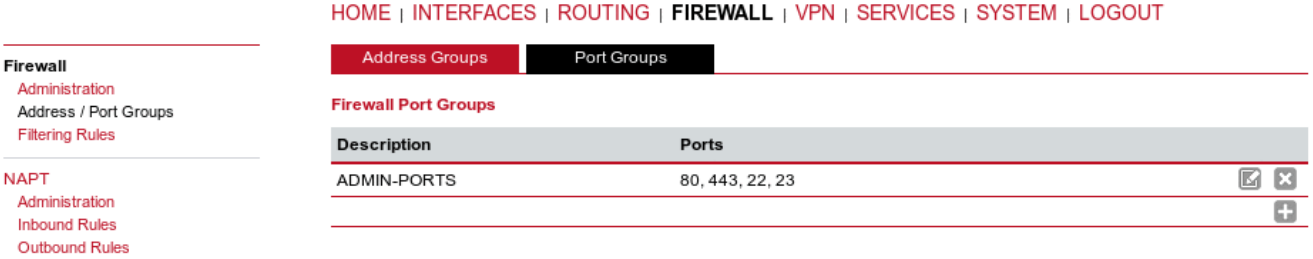
Administrative status: Enable or disable packet filtering.

Allow WAN administration: This option will predefine the rules for services on the WAN link as follows (TCP ports 80, 443, 22 and 23):

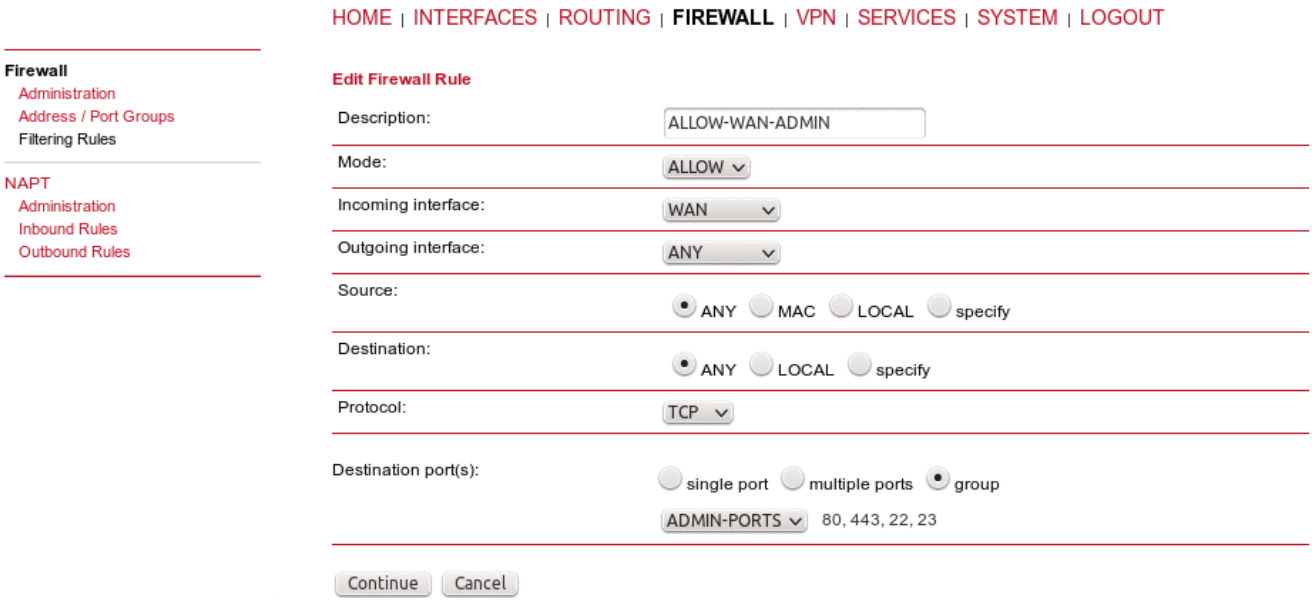


Address / Port Groups

This menu can be used to form address or port groups which can be later used for firewall rules in order to reduce the number of rules.



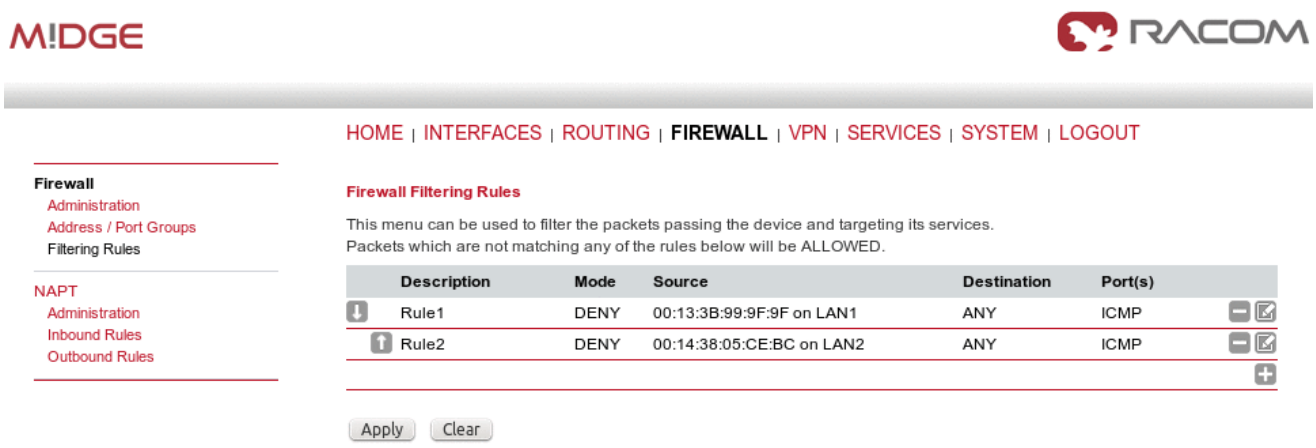
Add Firewall Rule



Description:	A meaningful description about the purpose of this rule.
Mode:	Whether the packets of this rule should be allowed or denied.
Incoming interface:	The Interface on which matching packets are received.
Outgoing interface:	The interface on which matching packets are received.
Source:	Source address of matching packets. Possible values are "ANY", "LOCAL" (addressed to the system itself), "Group" or "Specify" (specified by an address/netmask).
Destination:	The destination address of matching packets, can be "ANY", "LOCAL" (addressed ... itself), "Group" or "Specify (specified by address/netmask).
Protocol:	Used IP protocol of matching packets.
Destination port(s):	Destination port of matching packets. You can specify a single port or a range of ports here. Note that protocol must be set to UDP/TCP when using port filters.

Transparent Firewall

M!DGE/MG102i can be configured with its Ethernet interfaces being bridged. In this case, the transparent firewall functionality can be configured to limit reachability of individual hosts connected to M!DGE/MG102i based on their MAC addresses, i.e. units connected to ETH1 cannot communicate to units connected to ETH2.

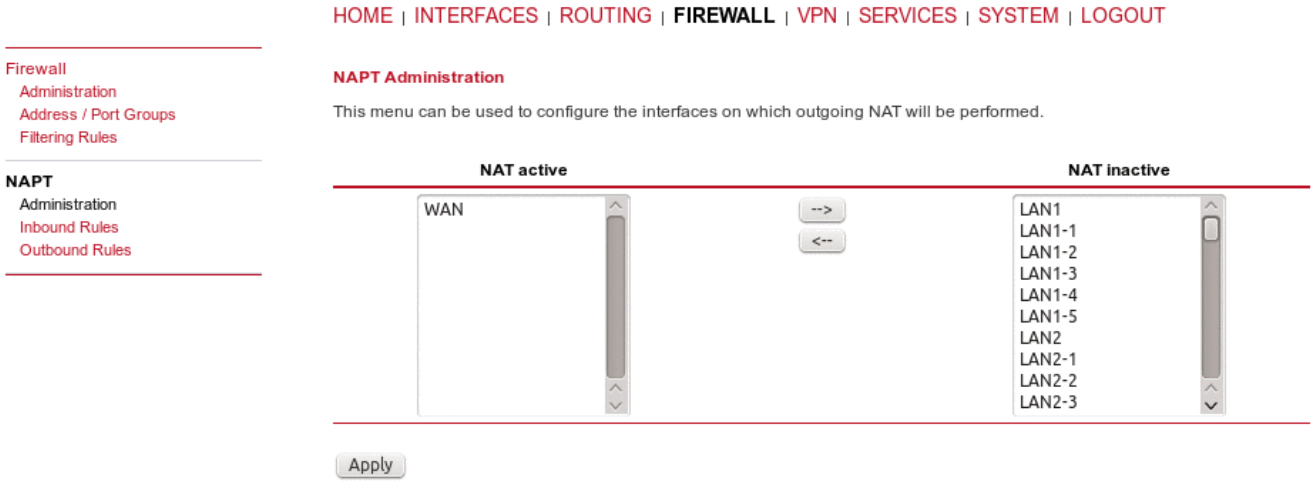


7.4.2. NAPT

This page allows setting of the options for Network Address and Port Translation (NAPT). NAPT translates IP addresses or TCP/UDP ports and enables communication between hosts on a private network and hosts on a public network. It generally allows a single public IP address to be used by many hosts from the private LAN network.

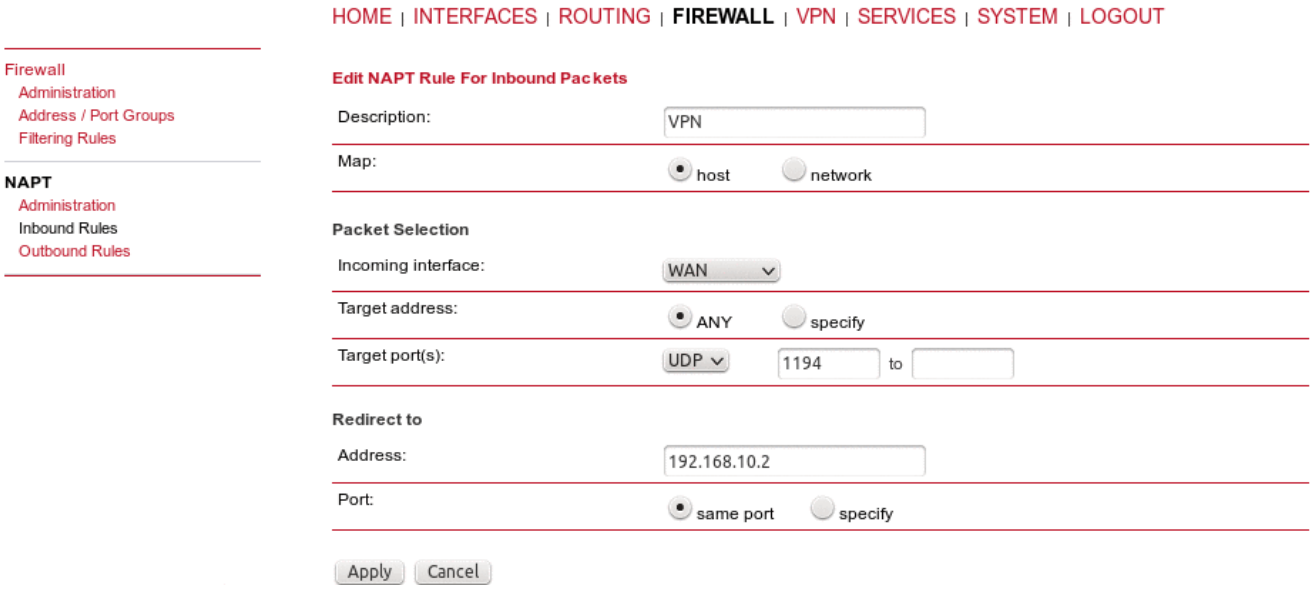
Administration

This menu can be used to configure the interfaces on which outgoing NAT will be performed.



Inbound Rules

Inbound rules can be used to modify the target section of IP packets and, for instance, forward a service or port to an internal host. By doing so, they will expose the service and make it reachable e.g. from the Internet. You may also establish 1:1 NAT to a complete host.



Description: A meaningful rule description

Incoming interface: Interface from which matching packets are received

Map: Choosing whether the rule applies to the host or to the network.

Target address: Destination address of matching packets (optional)

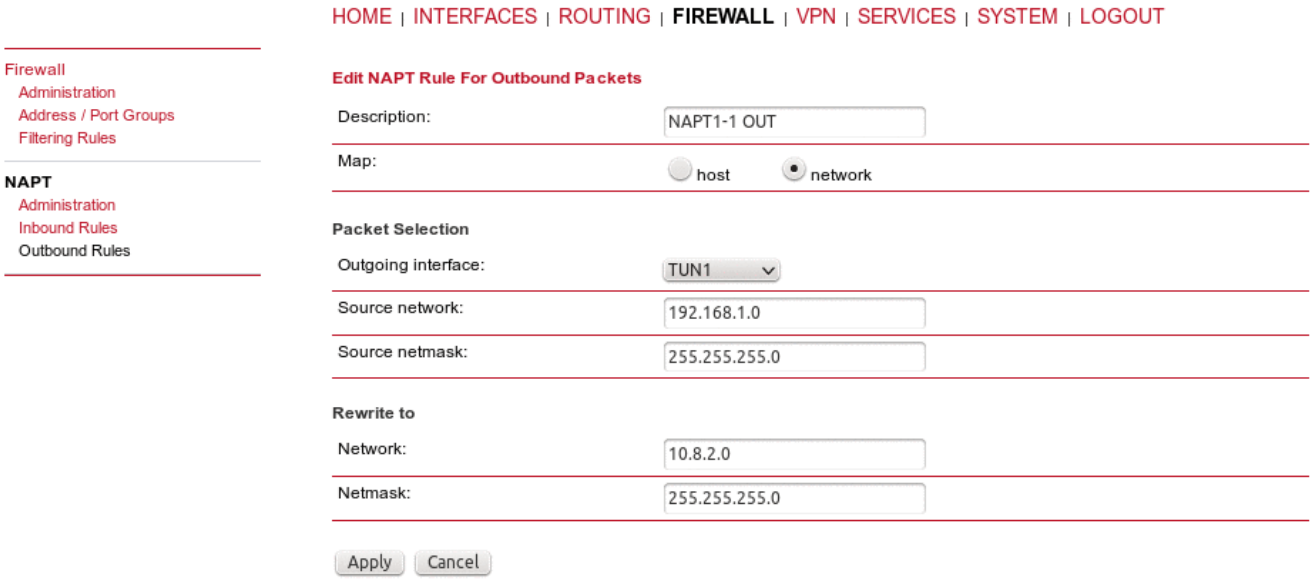
Target port(s): Used UDP/TCP port range of matching packets

Redirect to: Address or network/netmask to which matching packets will be redirected

Redirect port: Port to which matching packets will be targeted

Outbound Rules

Outbound rules will modify the source section of IP packets and can be for instance used for 1:1 NAT.



Description: A meaningful description of this rule

Map:	Choosing whether the rule applies to the host or to the network.
Outging interface:	Outgoing interface on which matching packets are leaving the router
Source address/ports:	Source address/ports of matching packets (if Map is set to "host")
Source network/netmask:	Source network/netmask of matching packets (if Map is set to "network")
Rewrite to address/port:	Address/port to which the source address/port of matching packets will be rewritten to
Rewrite to network/netmask:	Network/netmask to which the source network/netmask of matching packets will be rewritten to

7.5. VPN

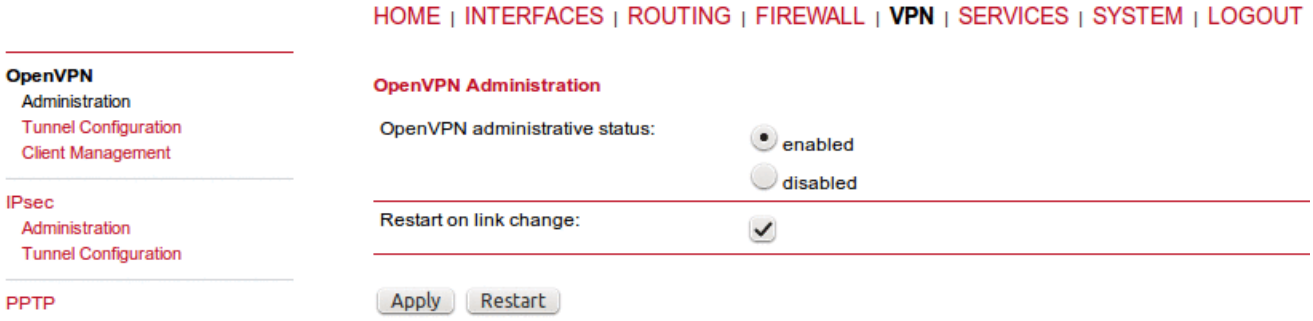
7.5.1. OpenVPN

Administration

OpenVPN administrative status: Enable or disable OpenVPN.

Restart on link change: If checked, the tunnel is restarted whenever any link changes the status.

If enabled, OpenVPN client configurations will be started whenever a WAN link has been established. Server configuration will be started immediately after after the bootup.

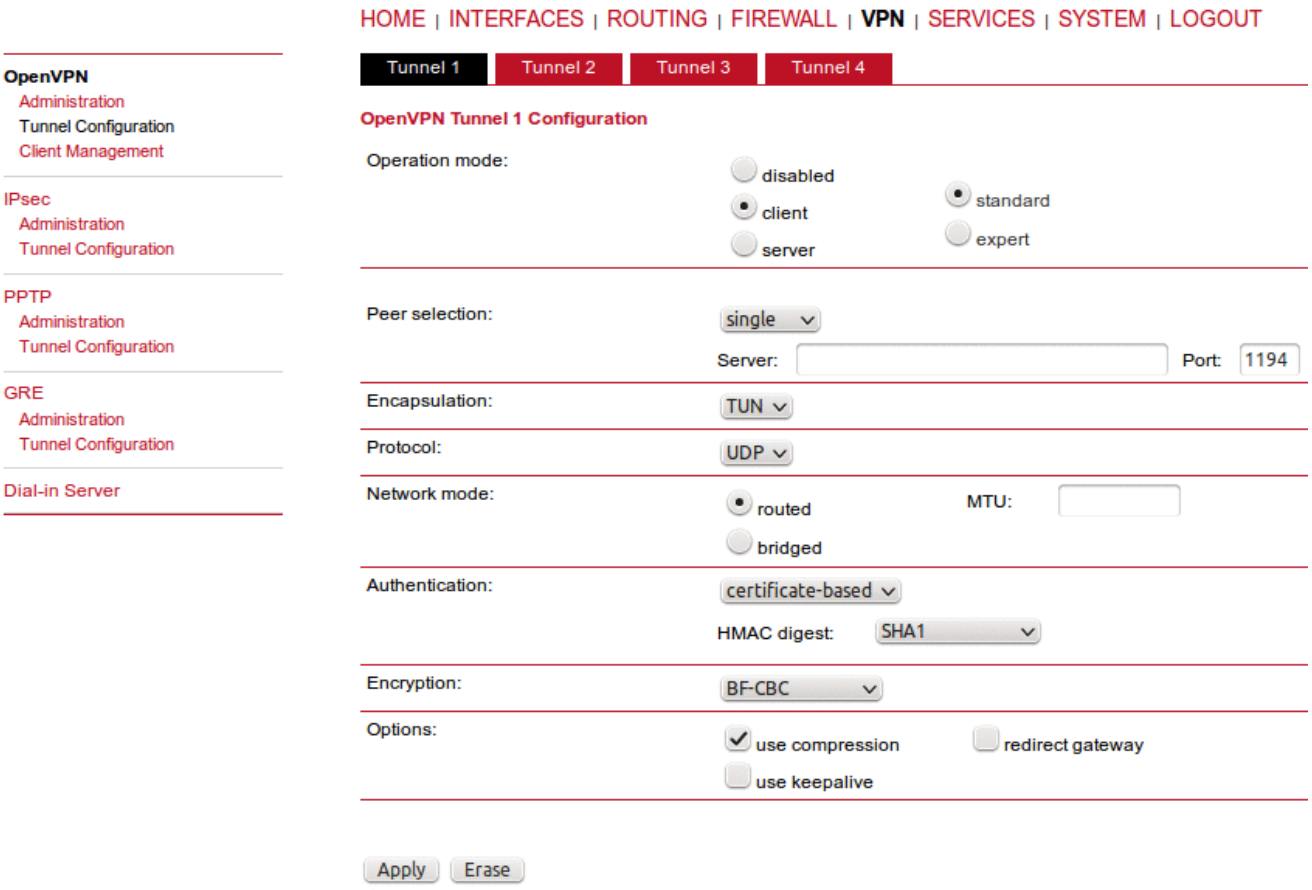


Tunnel Configuration

The router supports a single server tunnel and up to 4 client tunnels. You can specify tunnel parameters in standard configuration or upload an expert mode file which has been created in advance. Refer to section the section called “Client Management” to learn more about how to manage clients and generate the files.

Operation mode: Choose the client or server mode for this tunnel

Client Mode



Peer selection: Specifies how the remote peer shall be selected, besides a single server you may configure multiple servers which can , in case of failures, either be selected sequentially (i.e. failover) or randomly (i.e. load balancing).

Server The remote server address or hostname

Port The remote server port (1194 by default)

Encapsulation: The VPN device type which can be either TUN (typically used for routed connections) or TAP (used for bridged networks)

Protocol: The OpenVPN tunnel protocol to be used.

Network mode: Defines how the packets should be forwarded, can be routed or bridged from or to a particular interface. You can also set the MTU for the tunnel.

Authentication: You can choose between credential-based (where you have to specify a username and password) and certificate-based options. Note that keys/certificates have to be created in the SYSTEM -> Keys & Certificates menu. You may also upload files which you have generated on your host system.

HMAC digest: HMAC is commonly used message authentication algorithm (MAC) that uses a data string, a secure has algorithm, and a key, to produce a digital signature. OpenVPN's HMAC usage is to first encrypt a packet, then HMAC the resulting ciphertext. If OpenVPN receives a packet with a bad HMAC, it drops this packet. HMAC usually adds 16 or 20 Bytes per packet.

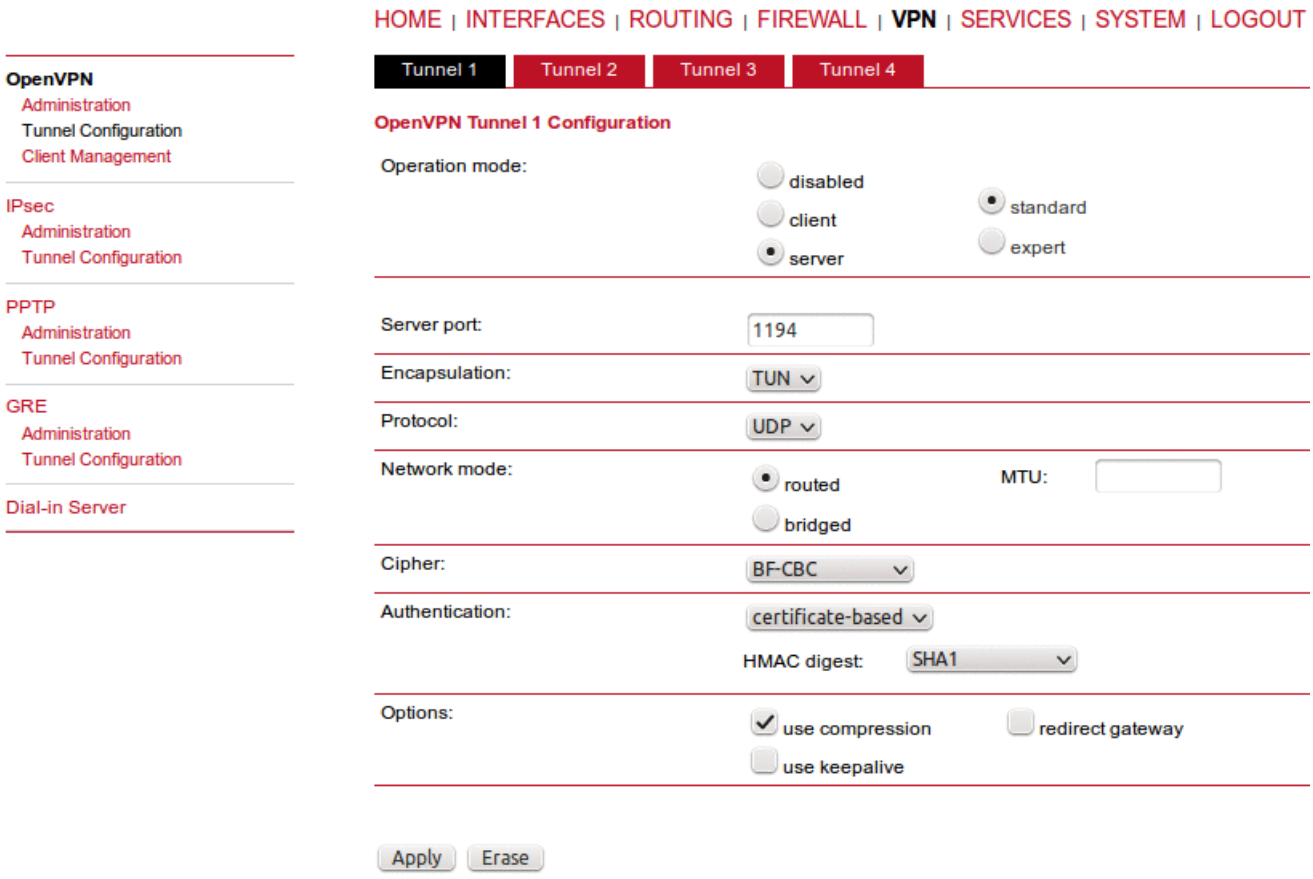
Encryption: Required cipher mechanism used for encryption.

Use compression: Enable or disable OpenVPN compression.

Use keepalive: Can be used to send a periodic keep alive packet in order to keep the tunnel up despite inactivity.

Redirect gateway: By redirecting the gateway, all packets will be directed to the VPN tunnel. Please ensure that essential services (such as DNS or NTP servers) can be reached via the network behind the tunnel. If in doubt, create an extra static route pointing to the correct interface.

Server Mode



A server tunnel typically requires the following files:

- server.conf (OpenVPN configuration file),
- ca.crt (root certificate file),
- server.crt (certificate file),
- server.key (private key file),
- dh1024.pem (Diffie Hellman parameters file),
- a directory (with default name “ccd”) containing client-specific configuration files.

Important

OpenVPN tunnels require a correct system time. Please ensure that all NTP servers are reachable. When using host names, a working DNS server is required as well.

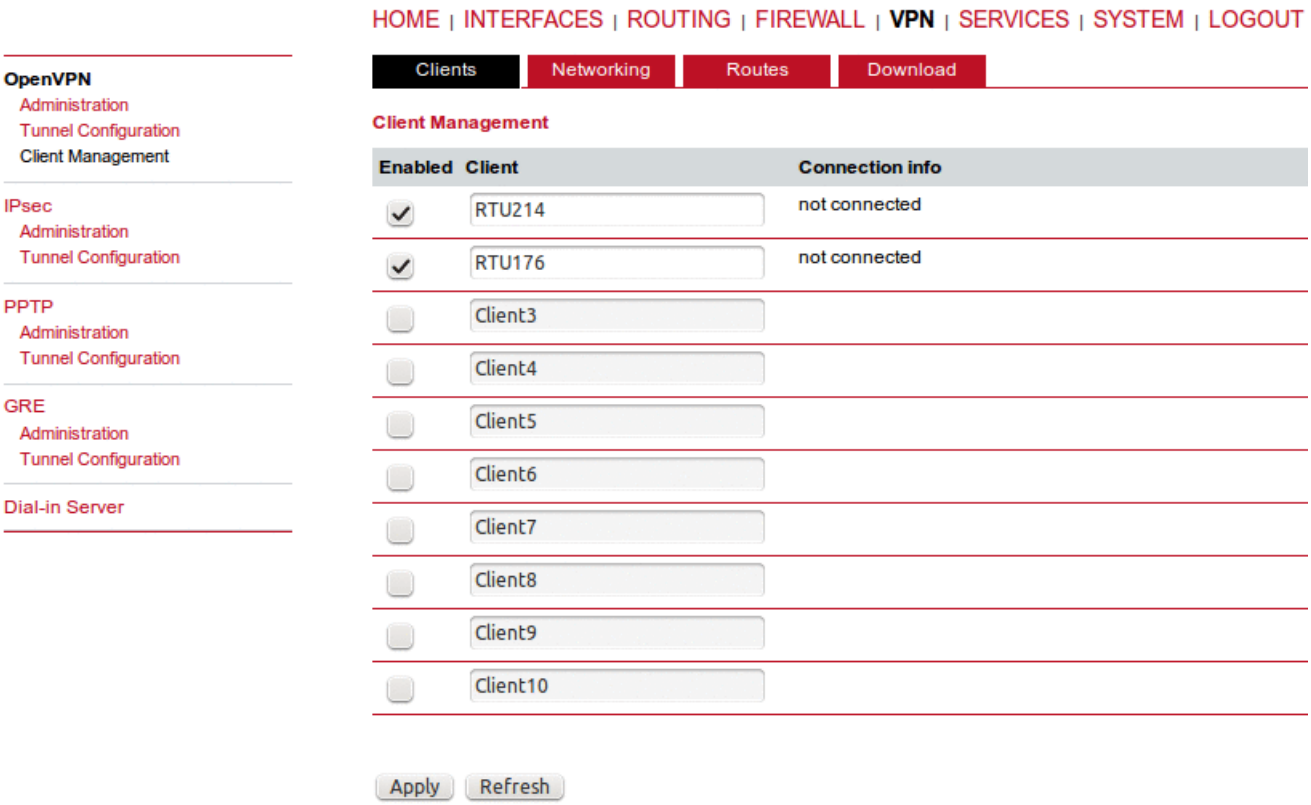
Client Management

Once you have successfully set up an OpenVPN server tunnel you can manage and enable clients which can connect to your service, the client's page also informs you about currently connected clients. Further, you can specify a fixed tunnel endpoint address of each client and its network behind. You can also define routes to be pushed to each client if you want to redirect traffic for particular networks towards the server and enable routing between clients.

Finally, you can generate and download all expert mode files to easily populate each client.

Note

The downloaded expert mode file needs to be unzipped and then individual client expert files can be uploaded to the respective routers.



Note

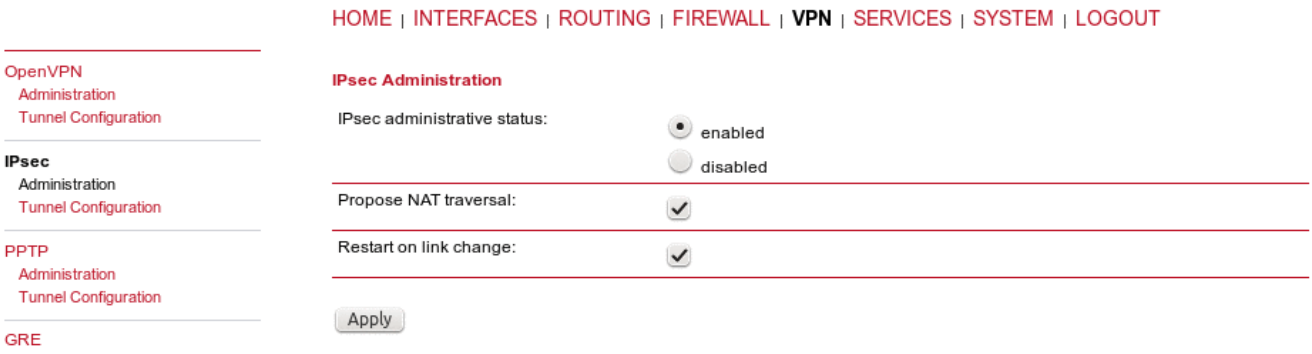
See the OpenVPN configuration example in our Application notes. (http://www.ra-com.eu/eng/products/m/midge/app/VPN_config.html#OpenVPN).

7.5.2. IPsec

IPsec is primarily used for securing the Internet communication by authenticating and/or encrypting IP packets within a data stream. IPsec includes various cryptographic protocols and ciphers for key ex-

change and data encryption and can be seen as one of the strongest VPN technologies in terms of security.

Administration

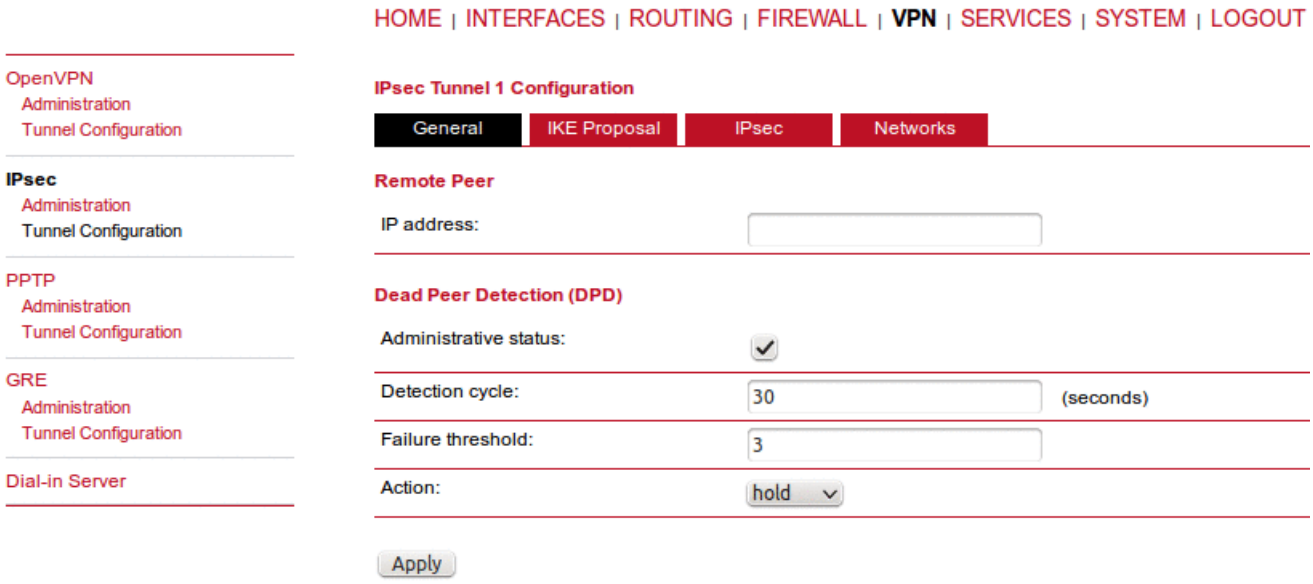


IPsec administrative status: Enable or disable IPsec

Propose NAT Traversal: NAT-Traversal is mainly used for connections which traverse a path where a router modifies the IP address/port of packets

Restart on link change: If checked, the tunnel is restarted whenever any link changes the status.

Configuration



General

Remote Peer IP address: The IPsec peer/responder/server IP address or host name

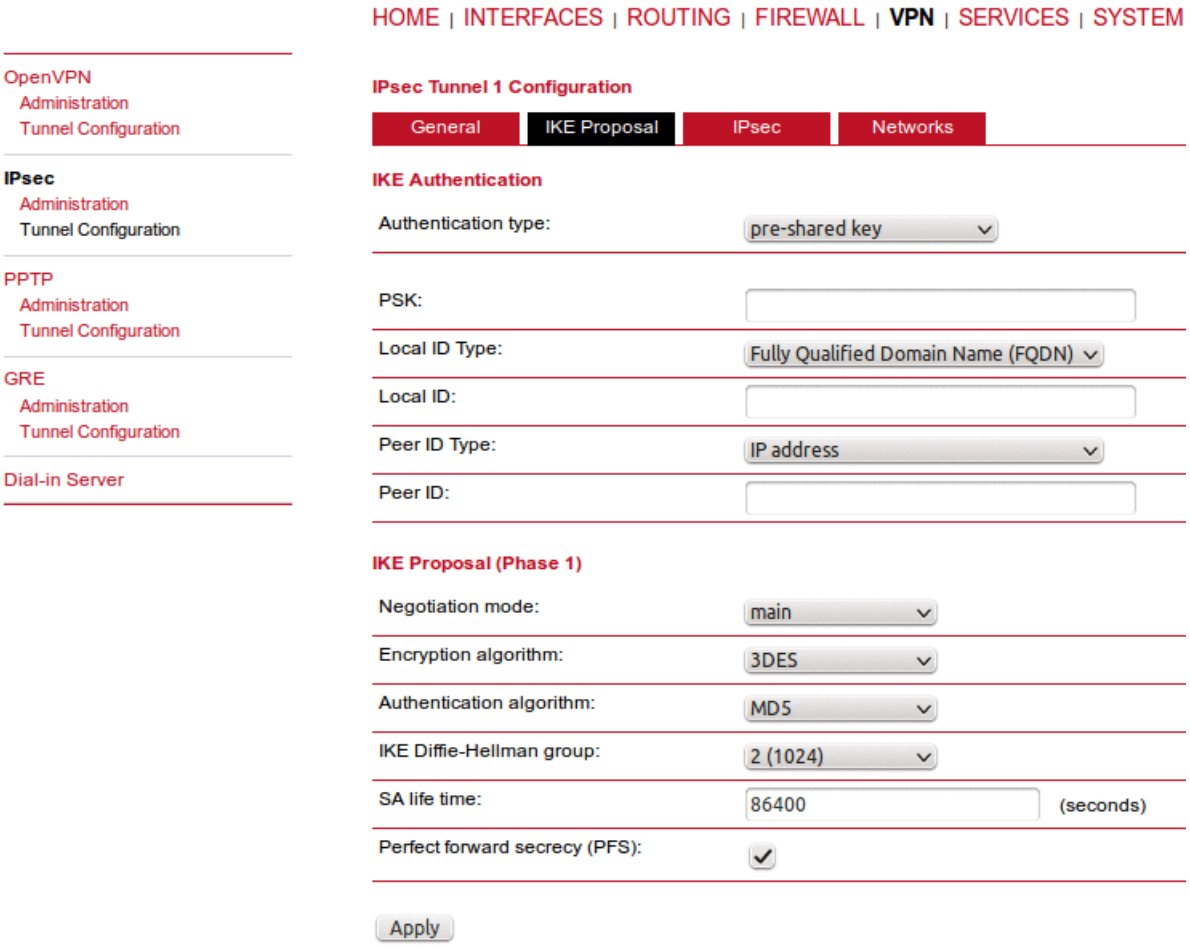
Administrative status: Enable or disable Dead Peer Detection. DPD will detect any broken IPSec connection, in particular the ISAKMP tunnel, and refresh the corresponding SAs (Security Associations) and SPIs (Security Payload Identifiers) for a faster tunnel re-establishment.

Detection cycle: Set the delay (in seconds) between Dead Peer Detection (RFC 3706) keepalives (R_U_THERE, R_U_THERE_ACK) that are sent for this connection (default 30 seconds)

Failure threshold: The number of unanswered DPD R_U_THERE requests until the IPsec peer is considered dead (the router will then try to re-establish a dead connection automatically)

Action: The action when a DPD enabled peer is declared dead. Hold (default) means the eroute is put into the hold status, while clear means the eroute and SA will both be cleared. Restart means that the SA will be immediately renegotiated.

IKE Proposal



RACOM routers support IKE authentication via the pre-shared keys (PSK) or certificates within a public key infrastructure.

Using PSK requires the following settings:

PSK: The pre-shared key used

Local ID Type: The identification type for the local router which can be FQDN, username@FQDN or IP address

Local ID: The local ID value

Peer ID type: The identification type for the remote router

Peer ID: The peer ID value

Note

When using certificates you would need to specify the Operation mode. When run as the PKI client you can create a Certificate Signing Request (CSR) in the certificates section which needs to be submitted at your Certificate Authority and imported to the router afterwards. In the PKI server mode the router represents the Certificate Authority and issues the certificates for remote peers.

Negotiation mode: Choose the negotiation mode (main, aggressive). The aggressive mode has to be used when dealing with dynamic endpoint addresses, but it is referred to be less secure compared to the main mode as it reveals your identity to an eavesdropper.

Encryption algorithm: The IKE encryption method (3DES, AES128, AES192, AES256)

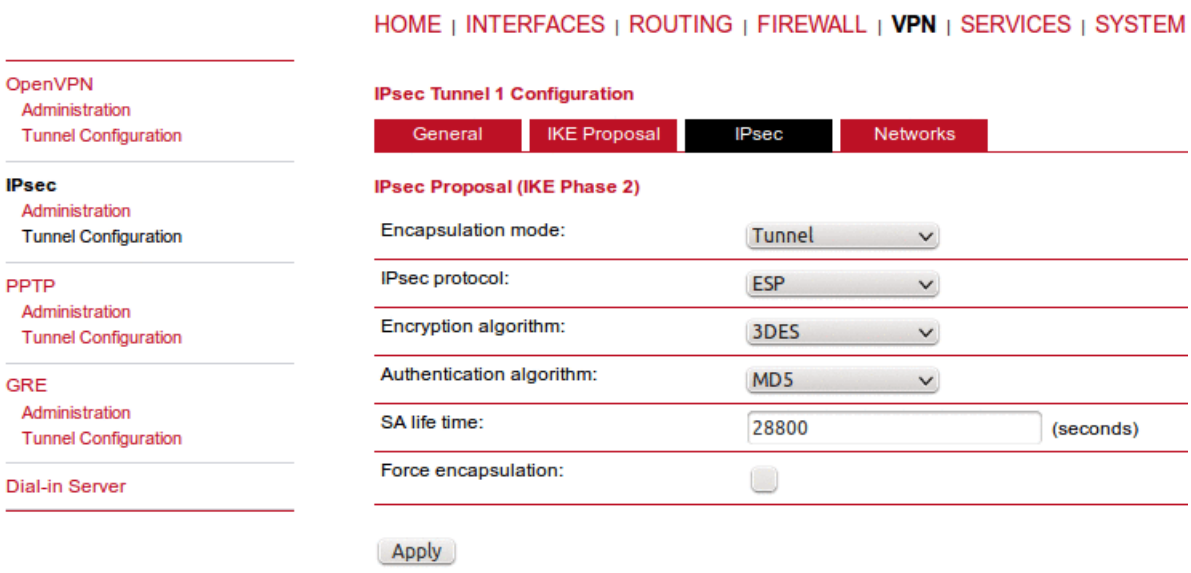
Authentication algorithm: The IKE authentication method (MD5, SHA1, SHA2-256)

IKE Diffie-Hellman group: The IKE Diffie-Hellman group (2, 5)

SA life time: The Security Association lifetime

Perfect forward secrecy (PFS): This feature heavily increases security as PFS avoids penetration of the key-exchange protocol and prevents compromising the keys negotiated earlier.

IPsec Proposal



Encapsulation mode: Only the tunnel encapsulation mode is enabled

IPsec protocol: Only the ESP IPsec protocol is enabled

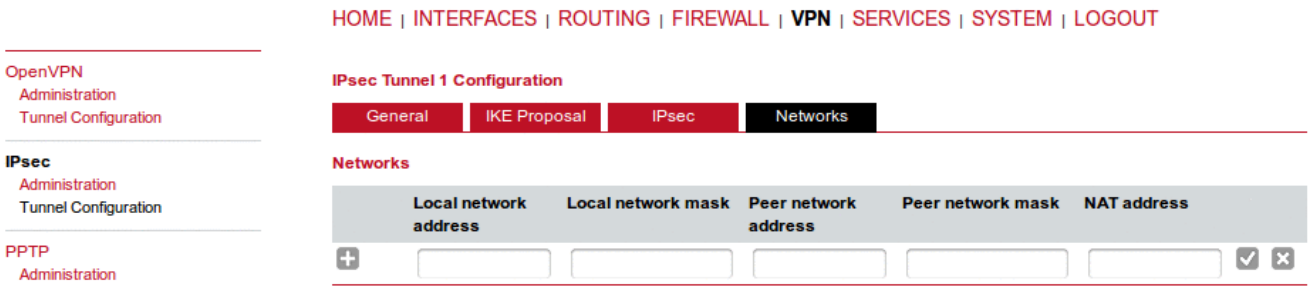
Encryption algorithm: The IKE encryption method (3DES, AES128, AES192, AES256)

Authentication algorithm: The IKE authentication method (MD5, SHA1, SHA2-256)

SA life time: The Security Association lifetime in seconds

Force encapsulation: Choose the negotiation mode (main, aggressive). The aggressive mode has to be used when dealing with dynamic endpoint addresses, but it is referred to be less secure compared to the main mode as it reveals your identity to an eavesdropper.

Networks



When creating Security Associations, IPsec keeps track of routed networks within the tunnel. Packets are only transmitted when a valid SA with the matching source and destination network is present. Therefore, you may need to specify the networks behind the endpoints by applying the following settings:

Local network address: The address of your Local Area Network (LAN)

Local network mask: The netmask of your LAN

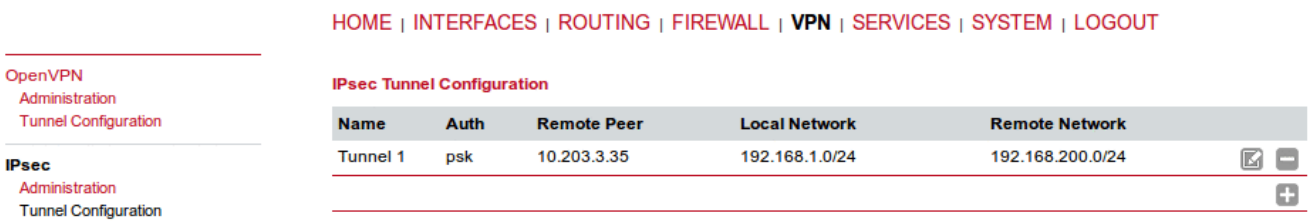
Peer network address: The address of the remote network behind the peer

Peer network mask: The netmask of the remote network behind the peer

NAT address: Optionally, you can apply NAT (masquerading) for packets coming from a different local network. The NAT address must reside in the network previously specified as the local network.

Note

Since the firmware 3.7.40.103, the maximum number of networks for individual IPsec tunnels has increased from 4 to 10.



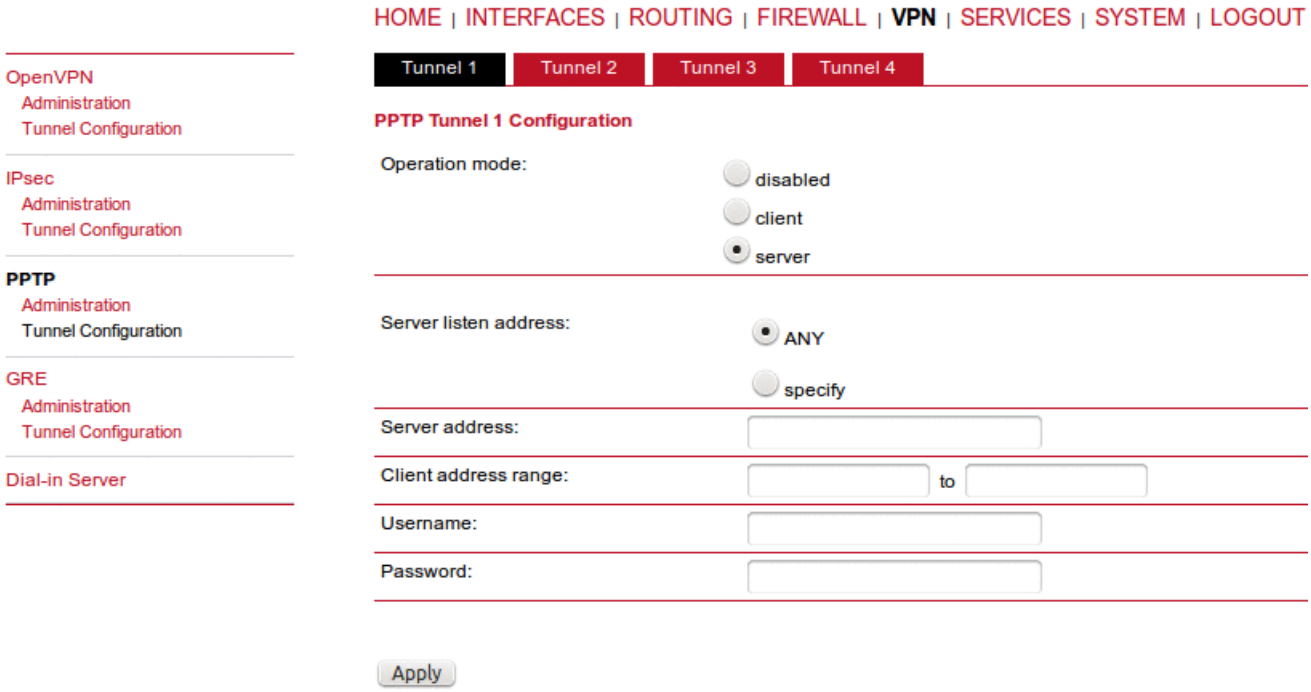
Note

See the IPsec configuration example in our Application notes (http://www.racom.eu/eng/products/m/midge/app/index.html), Chapter 2.2 IPsec[2].

[2] http://www.racom.eu/eng/products/m/midge/app/VPN_config.html#IPsec

7.5.3. PPTP

Point-to-Point Tunneling Protocol (PPTP) is a method for implementing virtual private networks between two hosts. PPTP is easy to configure and widely deployed amongst Microsoft Dial-up networking servers. However, it is nowadays considered insecure. When setting up a PPTP tunnel, you would need to choose between server or client.



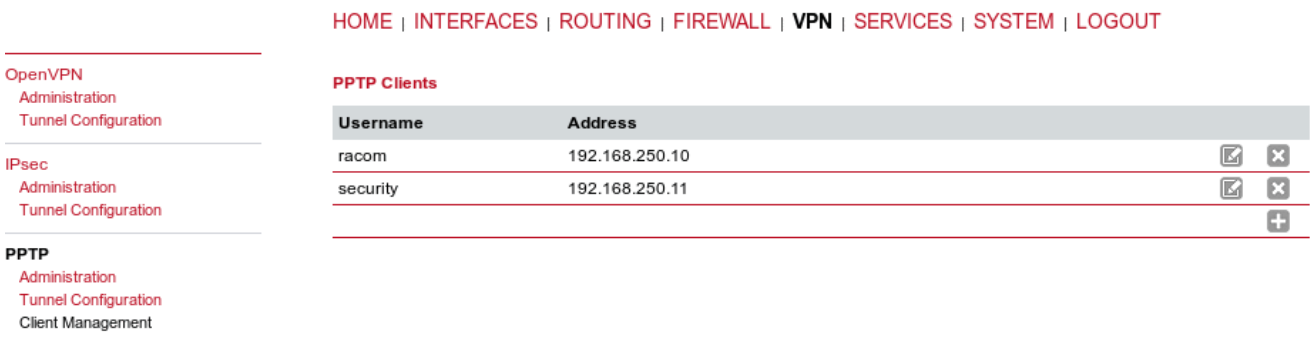
Listen address: Specifies on which IP address should be listened for incoming client connections

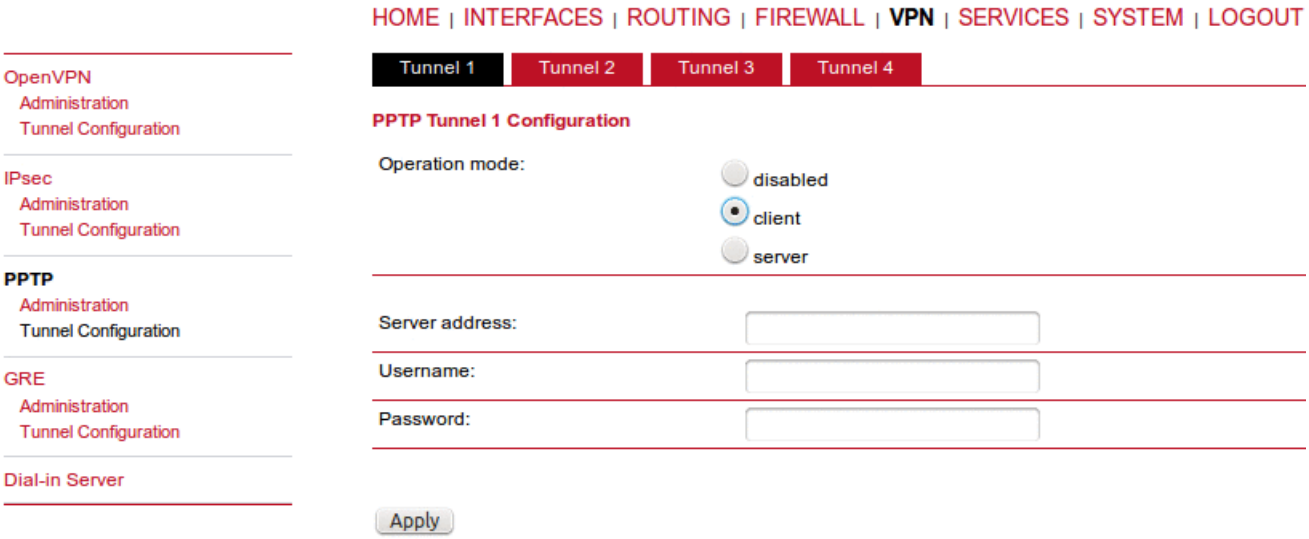
Server address: The server address within the tunnel

Client address range: Specifies a range of IP addresses assigned to each client

Username/password: The common username/password configuration

Once configured, individual clients can be configured with different credentials and IP addresses.





A client tunnel requires the following parameters to be set:

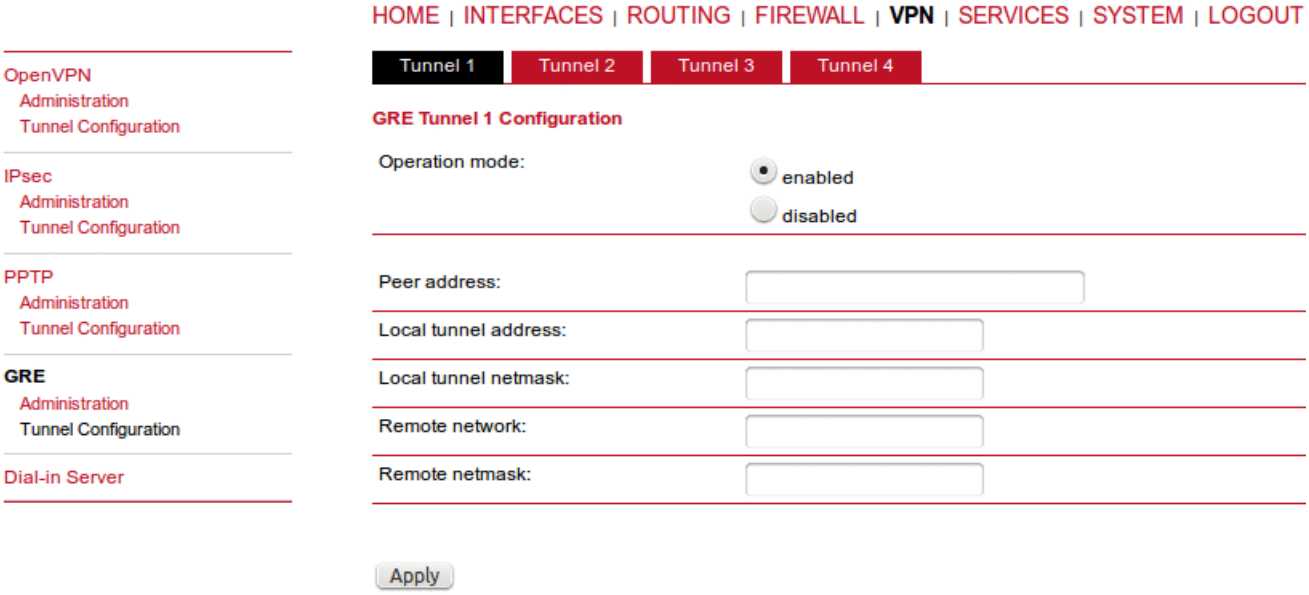
Server address: The address of the remote server

Username: The username used for authentication

Password: The password used for authentication

7.5.4. GRE

The Generic Routing Encapsulation (GRE) is a tunneling protocol that can encapsulate a wide variety of network layer protocols inside virtual point-to-point links over IP. GRE is defined in RFC 1701, 1702 and 2784. It does not provide encryption nor authorization but can be used on an address-basis on top of other VPN techniques (such as IPsec) for tunneling purposes.



The following parameters are required for setting up a tunnel:

Peer address The remote peer IP address

Local tunnel address	The local IP address of the tunnel
Local tunnel netmask	The local subnet mask of the tunnel
Remote network	The remote network address of the tunnel
Remote netmask	The remote subnet mask of the tunnel

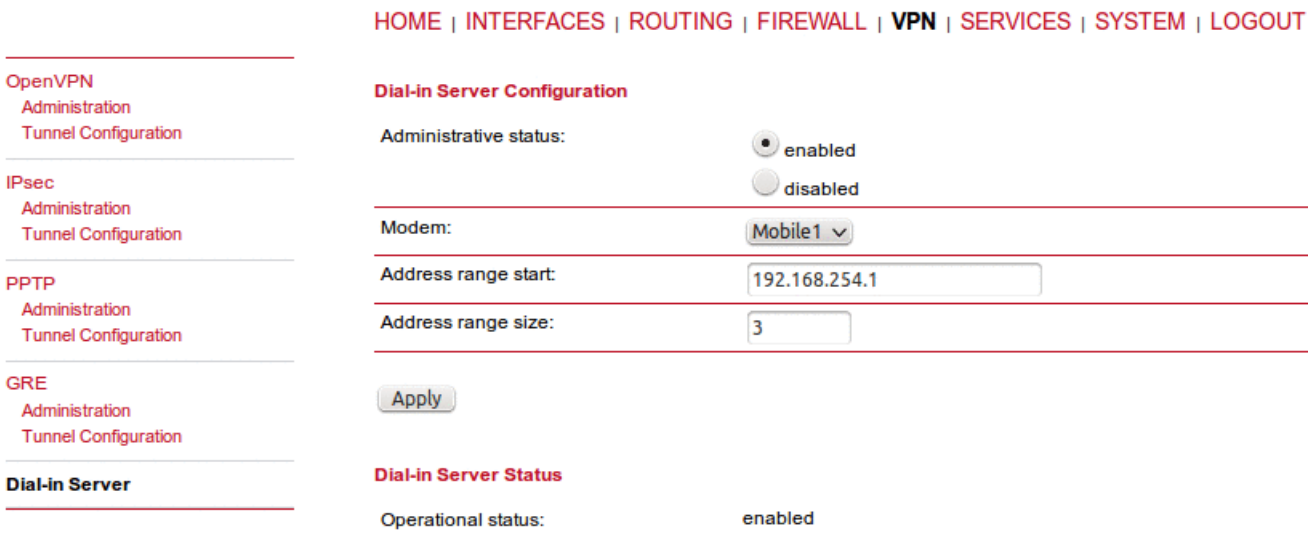
In general, the local tunnel address/netmask should not conflict with any other interface addresses. The remote network/netmask will result in an additional route entry in order to control which packets should be encapsulated and transferred over the tunnel.

7.5.5. Dial-in Server

On this page you can configure the Dial-in server in order to establish a data connection over GSM calls. Thus, one would generally apply a required service type of 2G-only, so that the modem registers to GSM only. Naturally, a concurrent use of mobile Dial-Out and Dial-In connection is not possible.

Note

The Dial-in Server is not supported by the M!DGE/MG102i LTE hardware.



Administrative status	Enabled/disabled - incoming call shall be /shall not be answered
Modem	Specifies the modem on which calls can come in
Address range start:	Start address of range of clients connecting to the dial-in server
Address range size:	Number of client addresses connecting to the server
Dial-in operational status:	Shows the current status of the connection

Besides the admin account you can configure further users in the user accounts section. which shall be allowed to dial-in. Please note that Dial-In connections are generally discouraged. As they are implemented as GSM voice calls, they suffer from unreliability and poor bandwidth.

7.6. SERVICES

7.6.1. SDK

RACOM routers are shipping with a Software Development Kit (SDK) which offers a simple and fast way to implement customer-specific functions and applications. It consists of:

1. An SDK host which defines the runtime environment (a so-called sandbox), that is, controlling access to system resources (such as memory, storage and CPU) and, by doing so, catering for the right scalability.
2. An interpreter language called arena, a light-weight scripting language optimized for embedded systems, which uses a syntax similar to ANSI-C but adds support for exceptions, automatic memory management and runtime polymorphism on top of that.
3. A RACOM-specific Application Programming Interface (API), which ships with a comprehensive set of functions for accessing hardware interfaces (e.g. digital IO ports, GPS, external storage media, serial ports) but also for retrieving system status parameters, sending E-Mail or SMS messages or simply just to configure the router.

Anyone, reasonably experienced in the C language, will find an environment that is easy to dig in. However, feel free to contact us via <support@racom.eu> and we will happily support you in finding a programming solution to your specific problem.

The Language

The arena scripting language offers a broad range of POSIX functions (like printf or open) and provides, together with tailor-made API functions, a simple platform for implementing any sort of applications to interconnect your favourite device or service with the router.

Here comes a short example:

```
/* This script prints short status and if the SMS section is setted properly, the status ▶
will be send even to your mobile phone :-)
 */

printf("------------------------------");
printf("\n\n");
printf(nb_status_summary(all));
printf("\n\n");
printf("------------------------------");

/* Please change the following number to your mobile phone number
 */
nb_sms_send("+420123456789", nb_status_summary(all));
```

A set of example scripts can be downloaded directly from the router, you can find a list of them in the appendix. The manual at menu SERVICES-Administration-Troubleshooting-SDK API gives a detailed introduction of the language, including a description of all available functions.

SDK API Functions

The current range of API functions can be used to implement the following features:

1. Send/Retrieve SMS
2. Send E-mail
3. Read/Write from/to serial device
4. Control digital input/output ports
5. Run TCP/UDP servers
6. Run IP/TCP/UDP clients
7. Access files of mounted media (e.g. an USB stick)
8. Retrieve status information from the system
9. Get or set configuration parameters
10. Write to syslog
11. Transfer files over HTTP/FTP
12. Perform config/software updates
13. Control the LEDs
14. Get system events, restart services or reboot system
15. Scan for networks in range
16. Create your own web pages
17. Voice control functions
18. SNMP functions
19. Various network-related functions
20. Other system-related functions

The SDK API manual at menu SERVICES-Administration-Troubleshooting-SDK API provides an overview but also explains all functions in detail.

Please note that some functions require the corresponding services (e.g. E-Mail, SMS) to be properly configured prior to utilizing them in the SDK.

Let's now pay some attention to the very powerful API function nb_status. It can be used to query the router's status values in the same manner as they can be shown with the CLI. It returns a structure of variables for a specific section (a list of available sections can be obtained by running cli status -h).

By using the dump function you can figure out the content of the returned structure:

```
/* Dump current WAN status */

dump ( nb_status ("wan") );
```

The script will then generate lines like maybe these:

```
struct(33): {
  .WANLINK1_GATEWAY = string[15]: "192.168.131.253"
  .WANLINK2_REGISTRATION_STATE = string[23]: "registeredInHomeNetwork"
  .WANLINK1_STATE = string[2]: "up"
  .WANLINK2_STATE_UP_SINCE = string[19]: "2015-06-10 14:41:59"
  .WANLINK1_STATE_UP_SINCE = string[19]: "2015-06-10 14:41:43"
  .WANLINK2_GATEWAY = string[11]: "10.64.64.64"
  .WANLINK1_DIAL_ATTEMPTS = string[1]: "0"
  .WANLINK2_SIGNAL_STRENGTH = string[3]: "-89"
  .WANLINK2_DATA_DOWNLOADED = string[7]: "1705494"
  .WANLINK2_DATA_UPLOADED = string[6]: "511619"
  .WANLINK1_DATA_UPLOADED = string[8]: "51587351"
  .WANLINK2_ADDRESS = string[11]: "10.203.3.28"
  .WANLINK2_NETWORK = string[7]: "O2 - CZ"
```

```
  .WANLINK1_DIAL_SUCCESS = string[1]: "1"
  .WANLINK1_ADDRESS = string[15]: "192.168.131.233"
  .WANLINK1_DOWNLOAD_RATE = string[3]: "202"
  .WANLINK2_SIM = string[4]: "SIM1"
  .WANLINK2_DOWNLOAD_RATE = string[1]: "8"
  .WANLINK1_UPLOAD_RATE = string[1]: "0"
  .WANLINK2_UPLOAD_RATE = string[1]: "8"
  .WANLINK2_DIAL_FAILURES = string[1]: "0"
  .WANLINK1_TYPE = string[3]: "eth"
  .WANLINK1_DIAL_FAILURES = string[1]: "0"
  .WANLINK2_DIAL_ATTEMPTS = string[1]: "1"
  .WANLINK2_MODEM = string[7]: "Mobile1"
  .WANLINK1_INTERFACE = string[4]: "LAN2"
  .WANLINK1_DATA_DOWNLOADED = string[8]: "95597767"
  .WAN_HOTLINK = string[8]: "WANLINK1"
  .WANLINK2_INTERFACE = string[5]: "WWAN1"
  .WANLINK2_SERVICE_TYPE = string[4]: "HSPA"
  .WANLINK2_DIAL_SUCCESS = string[1]: "1"
  .WANLINK2_TYPE = string[4]: "wwan"
  .WANLINK2_STATE = string[2]: "up"
}
```

In combination with the nb_config_set function, it is possible to start a re-configuration of any parts of the system upon status changes. You may find all possible parameters by reading the /etc/config/factory-config.cfg file accessible via CLI.

```
/etc/config $ cat factory-config.cfg | grep ntp
network.ntp.status                              =1
network.ntp.server0                             =0.pool.ntp.org
network.ntp.server1                             =1.pool.ntp.org
network.ntp.ping                                =1
network.ntp.interval                            =256
network.ntp.gpstime                             =0
network.ntp.access.0.address                    =192.168.1.0
network.ntp.access.0.netmask                    =255.255.255.0
network.ntp.access.1.address                    =
network.ntp.access.1.netmask                    =
network.ntp.access.2.address                    =
network.ntp.access.2.netmask                    =
```

Here is an example how one might adopt those functions:

```
/* Check the current NTP server and set it to the IP address 192.168.0.2
and enable the NTP synchronisation */

printf ("The NTP server was previously using IP address: ");
printf (nb_config_get("network.ntp.server0"));
printf("\n\n");

nb_config_set("network.ntp.server0=192.168.0.2");

if (nb_config_get ("network.ntp.status") == "0"){
```

```
  printf ("and was not running.");
  printf("\n\n");
  nb_config_set ("network.ntp.status=1");
}
else {
  printf ("and was running.");
  printf("\n\n");
}

printf ("The NTP server is now running with IP address: ");
printf (nb_config_get("network.ntp.server0"));
```

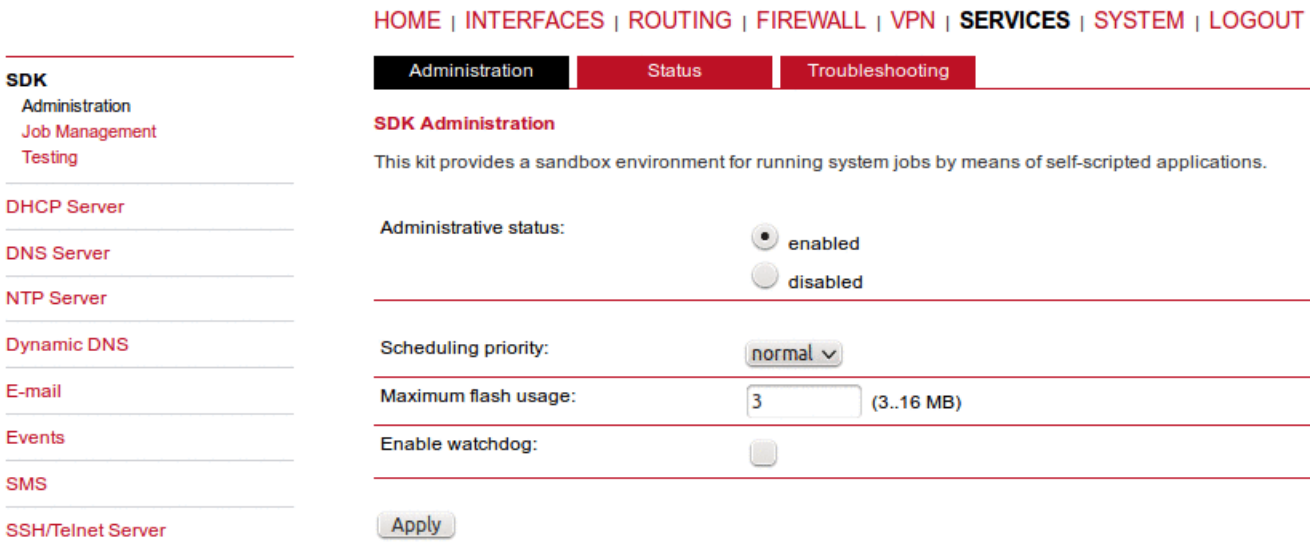
Running SDK

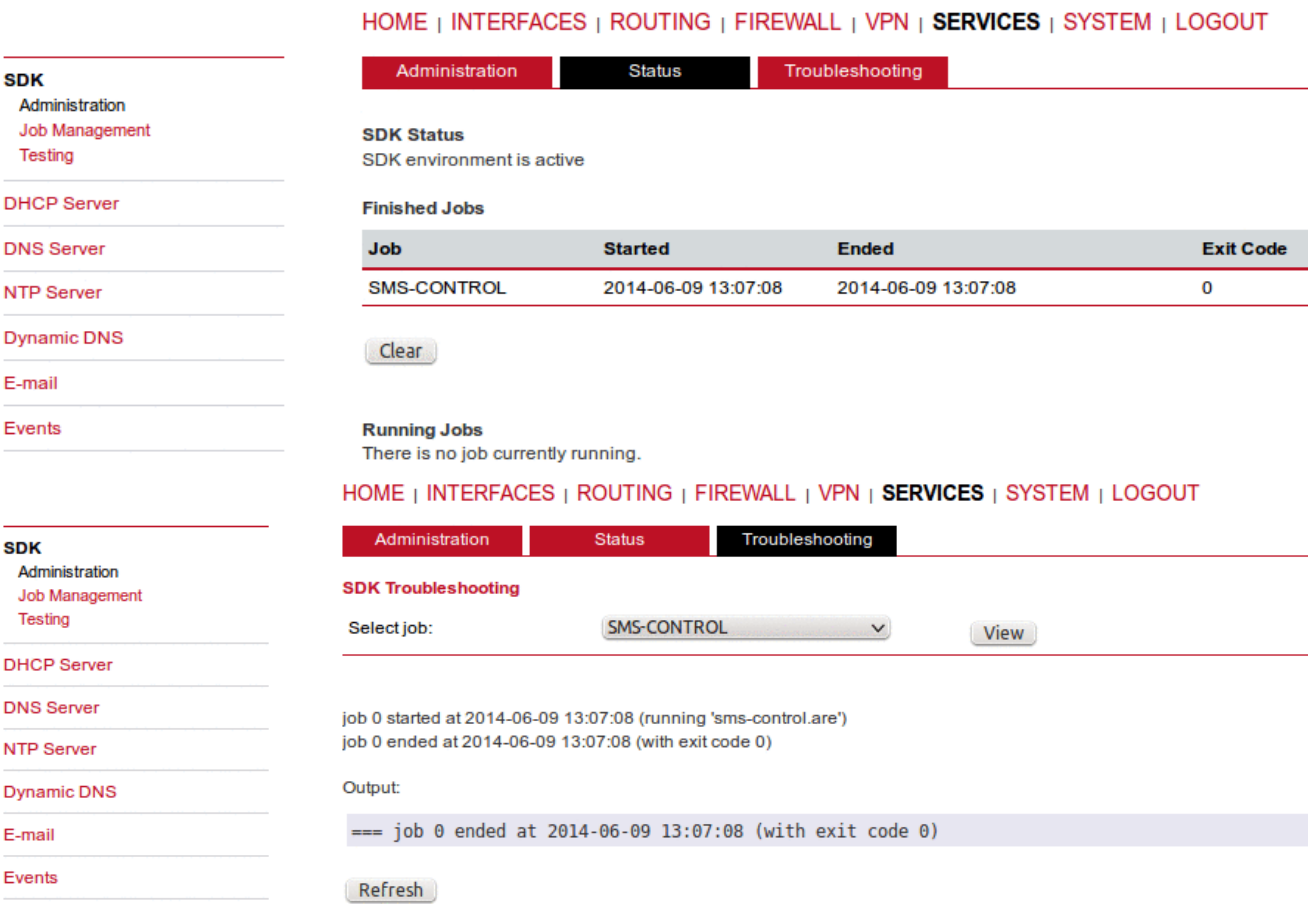
In the SDK, we are speaking of `scripts` and `triggers` which form `jobs`. Any `arena` script can be uploaded to the router or imported by using dedicated user configuration packages. You may also edit the script directly at the Web Manager or select one of our examples. You also have a testing section on the router which can be used to check your syntax or doing test runs.

Once uploaded, you will have to specify a trigger, that is, telling the router when the script is to be executed. This can be either time-based (e.g. each Monday) or triggered by one of the pre-defined system events (e.g. wan-up) as described in Section 7.6.7, “Events”. With both, a script and a trigger, you can finally set up an SDK job now. The test event usually serves as a good facility to check whether yourjob is working as expected. The admin section also offers facilities to troubleshoot any issues and control running jobs. The SDK host (sdkhost) corresponds to the daemon managing the scripts and their operations and thus avoiding any harm to the system. In terms of resources, it will limit CPU and memory for running scripts and also provide a pre-defined portion of the available flash storage. You may, however, extend it by external USB storage or (depending on your model) SD cards.

Files written to `/tmp` will be hold in the memory and will be cleared upon a script restart.. As your scripts operate in the sandbox, you will have no access to the system tools (such as `ifconfig`).

Administration





This page can be used to control the SDK host and apply the following settings:

Administrative status: Specifies whether SDK scripts should run or not

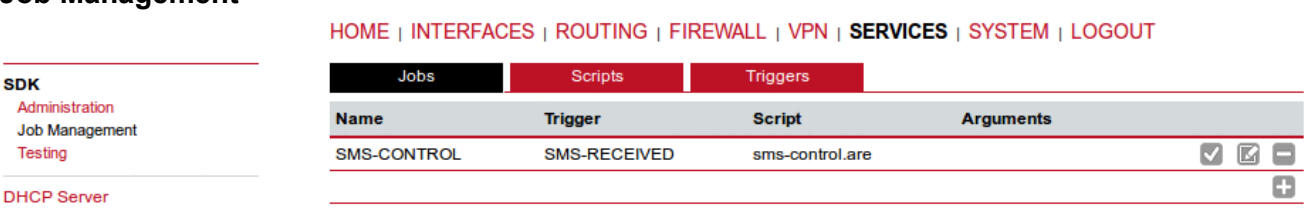
Scheduling priority: Specifies the process priority of the sdkhost, higher priorities will speed up scheduling your scripts, lower ones will have less impact to the host system

Maximum flash usage: The maximum amount of Mbytes your scripts can write to the internal flash

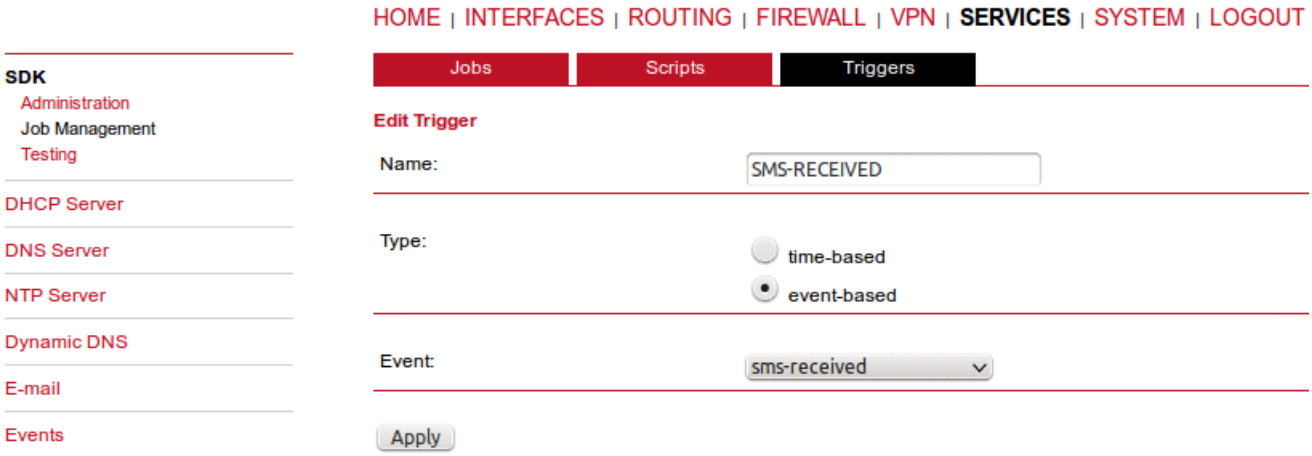
Enable watchdog: This option enables watchdog supervision for each script. If the script does not respond or is stopped with an exit code not equal null, the system is rebooted.

The status page informs you about the current SDK status. It provides an overview about any finished jobs, you can also stop a running job there and view the script output in the troubleshooting section where you will also find links for downloading the manuals and examples.

Job Management



This page can be used to set up scripts, triggers and jobs.



It is usually a good idea to create a trigger first which is made up by the following parameters:

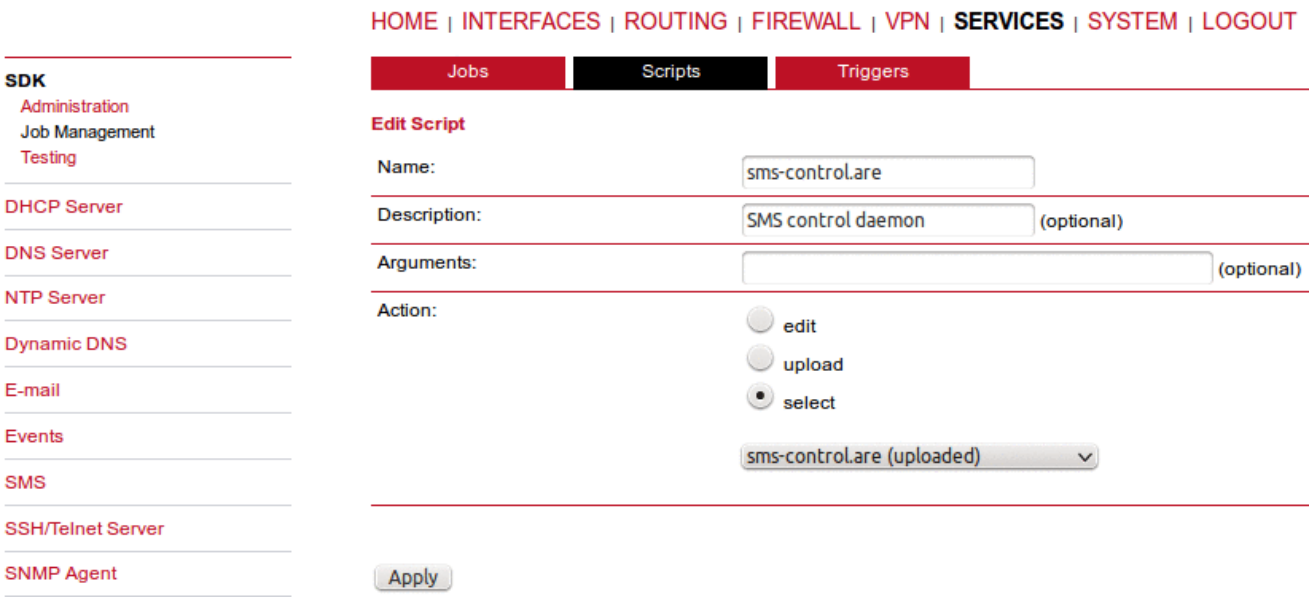
Name: A meaningful name to identify the trigger

Type: The type of the trigger, either time-based or event-based

Condition: Specifies the time condition for time-based triggers (e.g. hourly)

Timespec: The time specification which, together with the condition, specifies the `time(s)` when the trigger should be pulled

Event: The system event upon which the trigger should be pulled



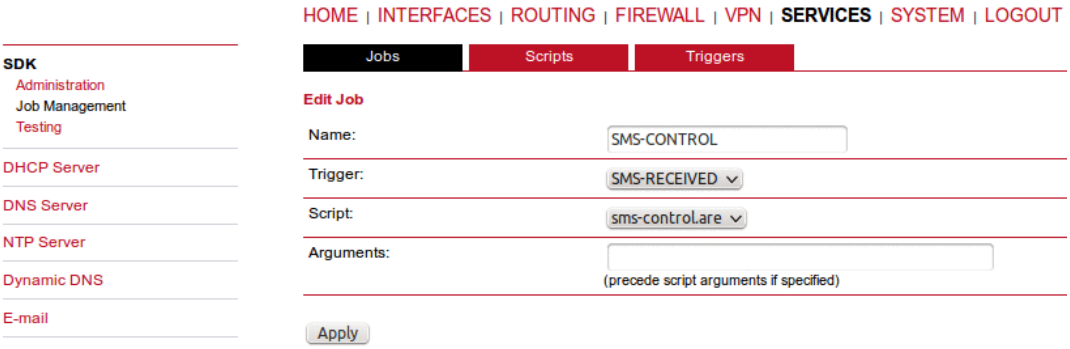
You can now add your personal script to the system by applying the following parameters:

Name: A meaningful name to identify the script

Description: An optional script description

Arguments: An optional set of arguments passed to the script (supports quoting)

Action: You may either edit a script, upload it to the system or select one of the example scripts or an already uploaded script



You are ready to set up a job afterwards, it can be created by using the following parameters:

Name: A meaningful name to identify the job

Trigger: Specifies the trigger that should launch the job

Script: Specifies the script to be executed

Arguments: Defines arguments which can be passed to the script (supports quoting), they will precede the arguments you formerly may have assigned to the script itself

Testing

```
/* Check the current NTP server and set it to the IP address 192.168.0.2
and enable the NTP synchronisation */

printf ("The NTP server was previously using IP address: ");
printf (nb_config_get("network.ntp.server0"));
printf("\n\n");

nb_config_set("network.ntp.server0=192.168.0.2");

if (nb_config_get ("network.ntp.status") == "0"){
  printf ("and was not running.");
  printf("\n\n");
  nb_config_set ("network.ntp.status=1");
}
else {
  printf ("and was running.");
  printf("\n\n");
}

printf ("The NTP server is now running with IP address: ");
printf (nb_config_get("network.ntp.server0"));
```

The testing page offers an editor and an input field for optional arguments which can be used to perform test runs of your script or test dedicated portions of it. Please note that you might need to quote arguments as they will otherwise be separated by white-spaces.

```
/* arguments : schnick schnack "s c h n u c k" */

for (i = 0; i < argc ; i++) {
    printf (" argv %d: %s\n", i, argv [i]);
}

/* generates:
* argv 0: /scripts/testrun
* argv 1: schnick
* argv 2: schnack
* argv 3: s c h n u c k
*/
```

In case of syntax errors, arena will usually print error messages as follows (indicating the line and position where the parsing error occurred):

```
/scripts/testrun:2:10:FATAL: parse error, unexpected $, expecting ';'
```

Note

It is now possible to upload SDK scripts into the Testing menu via browsing the required SDK script and clicking on the "Run" button.

SDK Sample Application

As an introduction, you can step through a sample application, namely the SMS control script, which implements remote control over short messages and can be used to send a system status back to the sender. The source code is listed in the appendix.

Once enabled, you can send a message to the phone number associated with a SIM / modem. It generally requires a password to be given on the first line and a command on the second, such as:

```
admin01
status
```

We strongly recommend to use authentication in order to avoid any unintended access, however you may pass noauth as argument to disable it. You can then skip the first line containing the password. Having a closer look to the script, you will see that you will also be able to restrict the list of permitted senders. Please inspect the system log for troubleshooting any issues.

The following commands are supported:

status — An SMS with the following information will be returned

- Signal strength
- Mobile connection state (up/down)
- current IP address of the mobile interface
- current IP address of the VPN interface (if enabled)

connect — This will initiate a Dial-out connection over GSM/UMTS and the VPN connection (if enabled) and trigger sending an SMS with the following information:

- current IP address of the PPP interface
- current IP address of the VPN interface (if enabled)

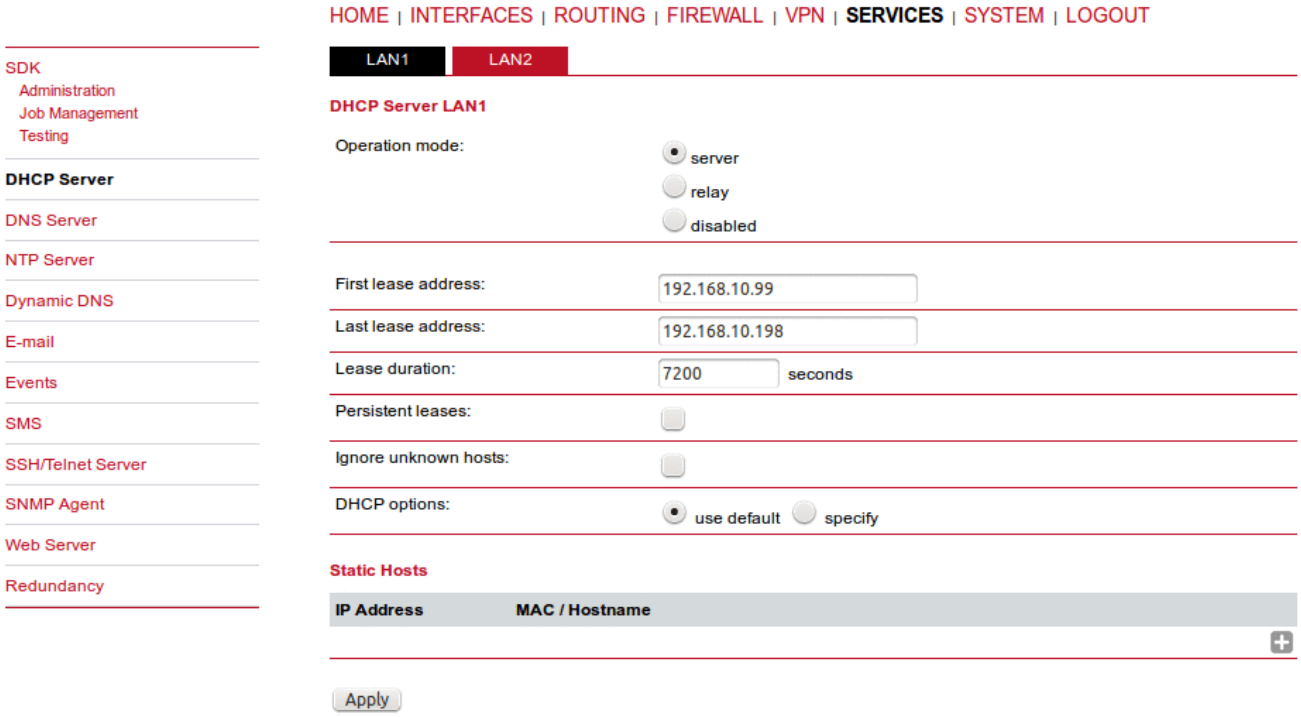
disconnect	terminates all WAN connections (including VPN)
reboot	Initiates a system reboot
output 1 on	Switch digital output 1 on
output 1 off	Switch digital output 1 off
output 2 on	Switch digital output 2 on
output 2 off	Switch digital output 2 off

A response to the status command typically looks like:

```
System: MIDGE midge (0002A9FFC32E)
WAN1: WWAN1 is up (10.204.8.3, Mobile1,
HSPA, -65 dBm, LAI 23003)
DIO: IN1=off, IN2=off, OUT1=off, OUT2=on
```

7.6.2. DHCP Server

This section can be used to individually configure a DHCP service for each LAN interface.



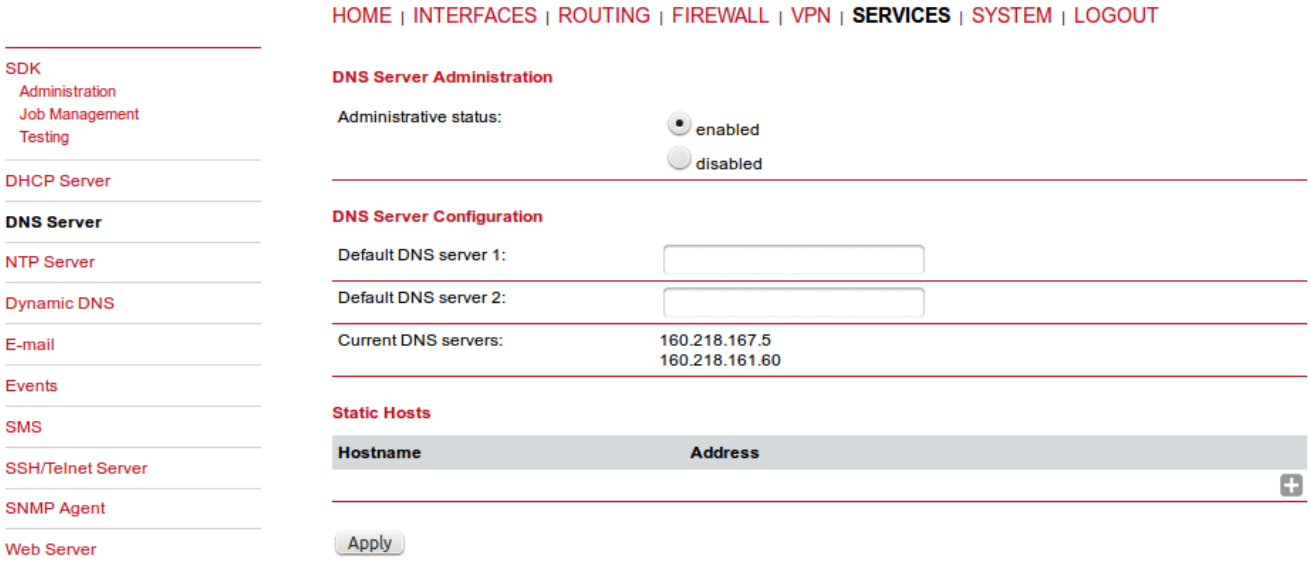
Operational mode: The DHCP operational mode can be disabled or set to the "server" or "relay" mode. As a server, the unit answers to DHCP requests from hosts in the LAN directly. Aa a relay, the unit resends the requests to the configured DHCP server which handles them.

First lease address: First address for DHCP clients

Last lease address:	Last address for DHCP clients
Lease duration:	Number of seconds (30-86400) how long a given lease will be valid until it has to be requested again
Persistent leases:	By turning this option on, router will remember to give leases even after a reboot. It can be used to ensure the same IP addresses are assigned to a particular host.
Ignore unknown hosts:	By checking this option, only static hosts will obtain the IP leases
DHCP options:	By default DHCP will hand out the interface address as the default gateway and DNS server address if not configured elsewhere. It is possible to specify different addresses here.
Static Hosts:	The option to add a static host configured with the IP address, MAC address and/or hostname.

7.6.3. DNS Server

The DNS server can be used to proxy DNS requests towards servers on the net which have for instance been negotiated during WAN link negotiation. By pointing DNS requests to the router, one can reduce outbound DNS traffic as it is caching already resolved names but it can be also used for serving fixed addresses for particular host names.

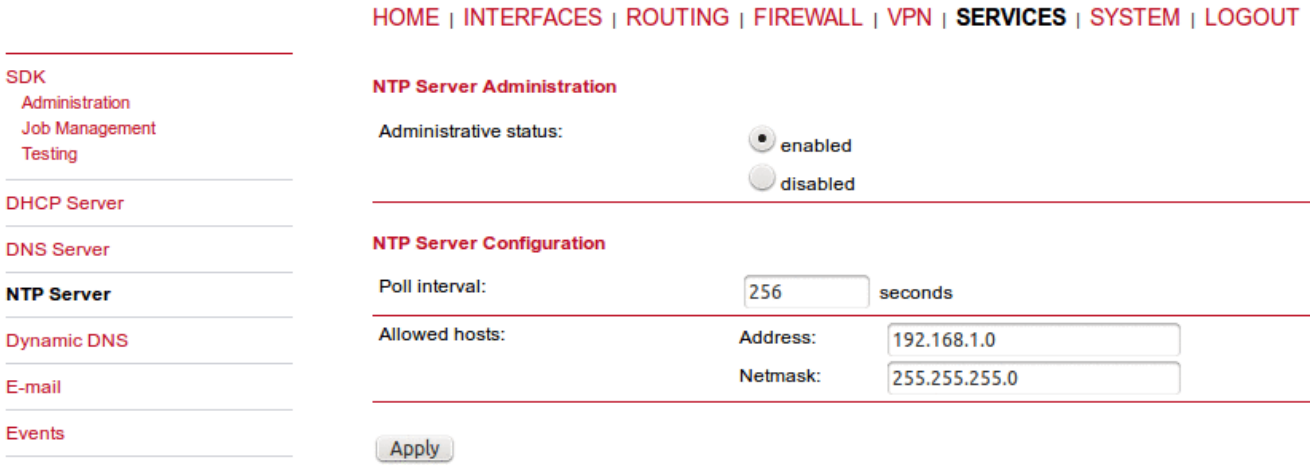


Administrative status:	Enabled or disabled
Default DNS server 1:	The primary DNS server to be queried
Default DNS server 2:	The secondary server which will be used in case the primary server is not available.

You may further configure static hosts for serving fixed IP addresses for various hostnames. Please remember to point local hosts to the router's address for resolving them.

7.6.4. NTP Server

This section can be used to individually configure the Network Time Protocol (NTP) server function.



Administrative status: Enabled or disabled

Poll interval: Defines the polling interval (64-4096 seconds) for synchronizing the time with the master clock servers

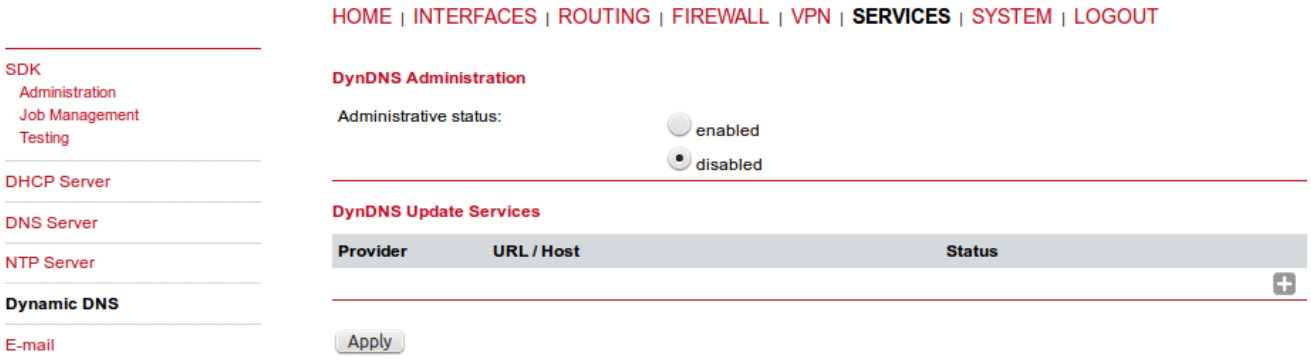
Allowed hosts: Defines the IP address range which is allowed to poll the NTP server

Note

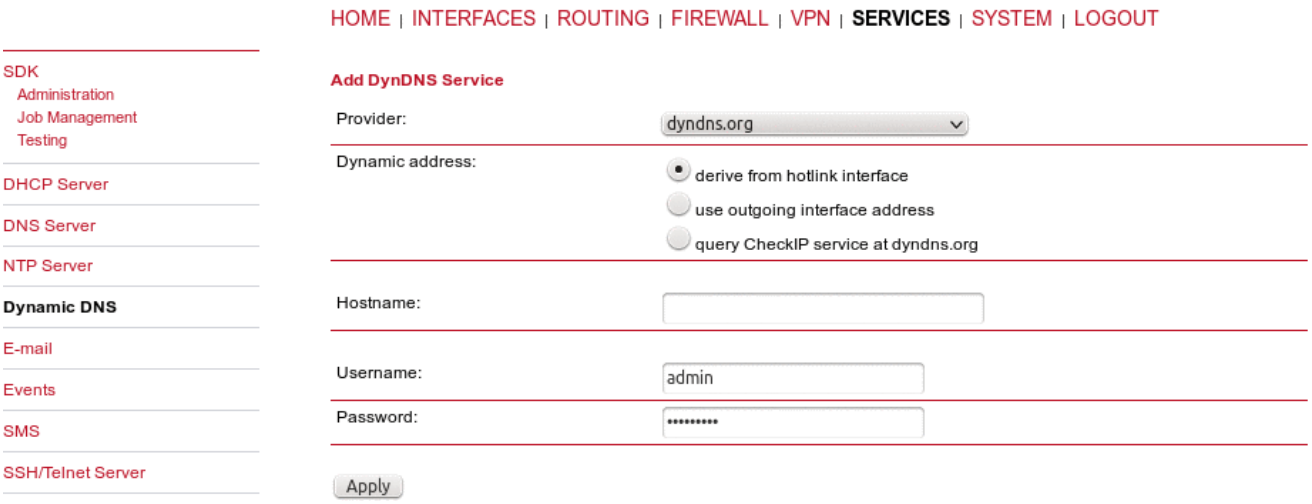
See the description of how to set the correct router time in the section called “Time & Region”.

7.6.5. Dynamic DNS

Dynamic DNS client on this box is generally compatible with various DynDNS services on the Internet running by means of definitions by the DynDNS organization (see www.dyndns.com for server implementations).



Administrative status: Enabled or disabled



Dynamic address: Specifies whether the address is derived from the hotlink, outgoing interface address or via an external service. Usually, the hotlink option is used.

Hostname: The host-name provided by your DynDNS service (e.g. mybox.dyndns.org)

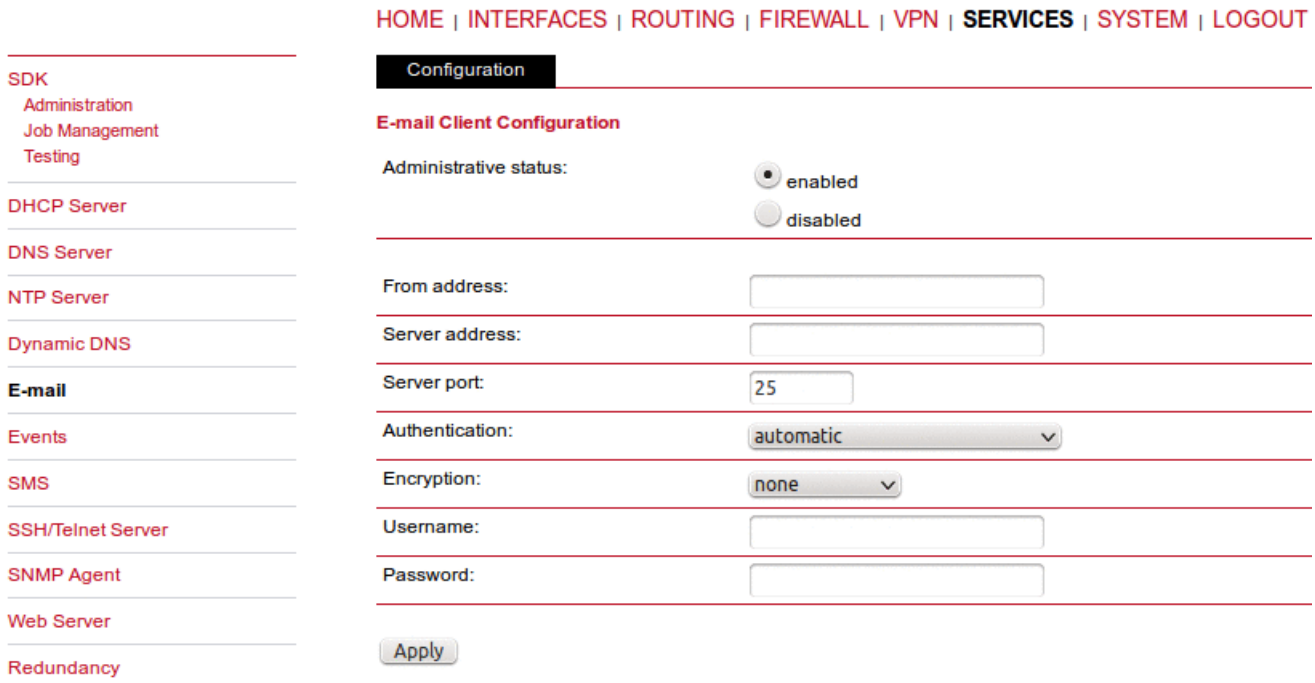
Username: The user-name used for authenticating at the service

Password: The password used for authentication

Please note that your RACOM router can operate as DynDNS service as well, provided that you hold a valid SERVER license and have your hosts pointed to the DNS service of the router.

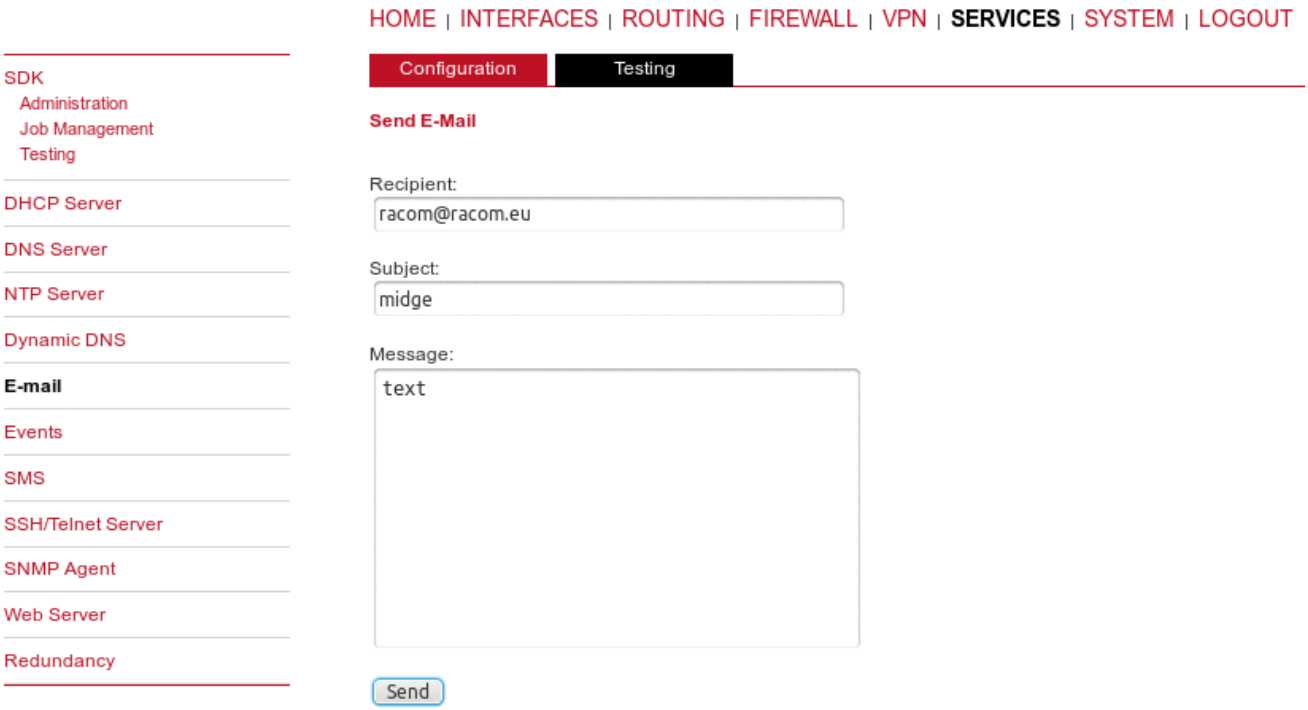
7.6.6. E-mail client

The E-Mail client can be used to send notifications to a particular E-Mail address upon certain events or by SDK scripts.



Administrative status: E-mail client administrative status - enabled or disabled

From address:	Sender e-mail address
Server address:	SMTP server address
Server port:	SMTP server port (typically 25)
Authentication:	Choose the required authentication method to authenticate against the SMTP server
Encryption:	The optional encryption for the e-mail messaging (none or TLS)
Username:	User name for authentication
Password:	Password for authentication



After configuring E-mail successfully, you can also test e-mail messages.

7.6.7. Events

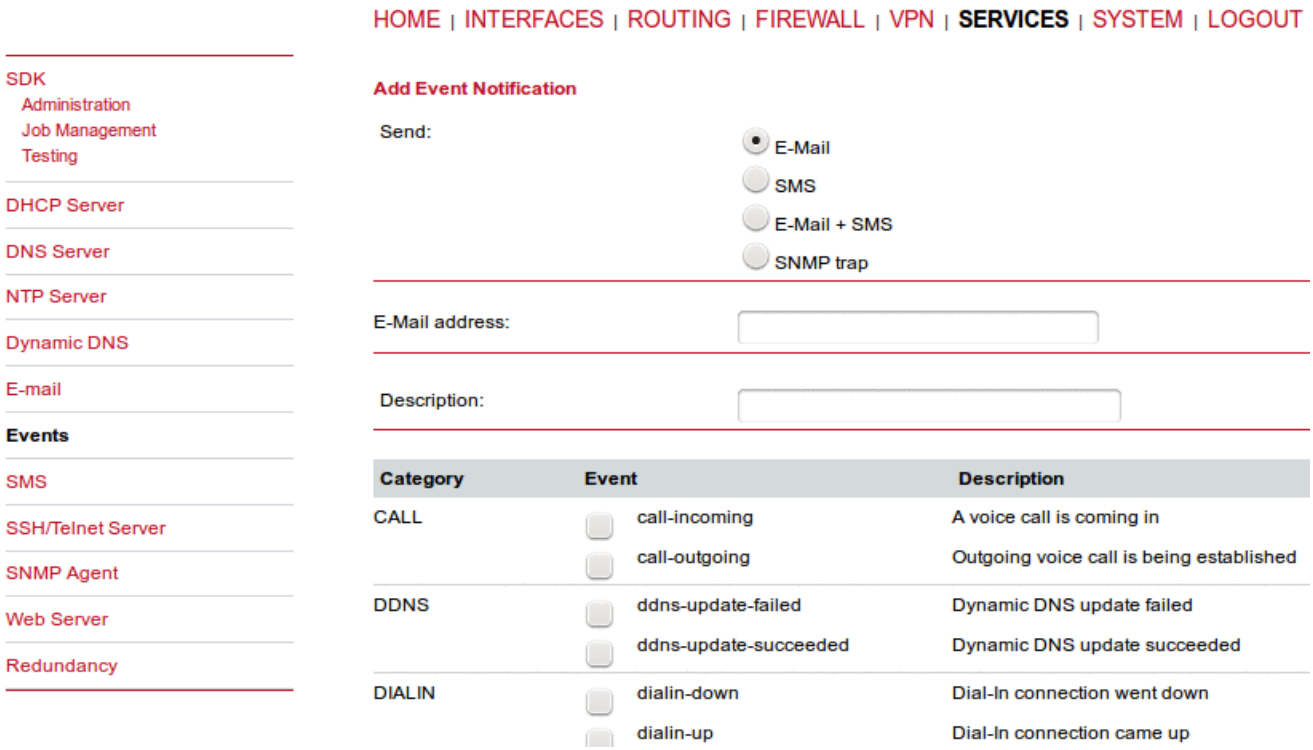
By using the event manager you can notify one or more recipients by SMS or E-Mail upon certain system events. These messages will contain a description provided by you and a short system info.

Additionally, you can choose the SNMP trap to be sent upon these events. Each event trap has its own OID - .1.3.6.1.4.1.33555.1.100.0.X.0.X where X is trap related. See the descriptions of the events below for the specific OID numbers. Please contact our technical department for more details.

Note

Own traps can be configured via SDK. See SDK script examples.

Events



The default texts for a specific Event are as follows:

Category	Event (ID)	Description
CALL	call-incoming (701)	A GSM call is coming in
	call-outgoing (702)	Outgoing voice call is being established
DDNS	ddns-update-failed (802)	Dynamic DNS update failed
	ddns-update-succeeded (801)	Dynamic DNS update succeeded
DIALIN	dialin-down (409)	Dial-In connection went down
	dialin-up (408)	Dial-In connection came up
DIO	dio-in1-off (202)	DIO IN1 turned off
	dio-in1-on (201)	DIO IN1 turned on
	dio-in2-off (204)	DIO IN2 turned off
	dio-in2-on (203)	DIO IN2 turned on
	dio-out1-off (206)	DIO OUT1 turned off
	dio-out1-on (205)	DIO OUT1 turned on
	dio-out2-off (208)	DIO OUT2 turned off
	dio-out2-on (207)	DIO OUT2 turned on
GPS	gps-down (302)	GPS signal is not available
	gps-up (301)	GPS signal is available
GRE	gre-down (413)	GRE connection went down
	gre-up (412)	GRE connection came up
IPSEC	ipsec-down (404)	IPsec connection went down
	ipsec-up (403)	IPsec connection came up

Category	Event (ID)	Description
MOBILEIP	mobileip-down (411)	Mobile IP connection went down
	mobileip-up (410)	Mobile IP connection came up
OPENVPN	openvpn-down (402)	OpenVPN connection went down
	openvpn-up (401)	OpenVPN connection came up
PPTP	pptp-down (407)	PPTP connection went down
	pptp-up (406)	PPTP connection came up
SDK	sdk-startup (507)	SDK has been started
SMS	sms-notsent (602)	SMS has not been sent
	sms-received (603)	SMS has been received
	sms-report-received (604)	SMS report has been received
	sms-sent (601)	SMS has been sent
SYSTEM	system-login-failed (501)	User login failed
	system-login-succeeded (502)	User login succeeded
	system-logout (503)	User logged out
	system-rebooting (504)	System reboot has been triggered
	system-startup (505)	System has been started
	system-time-updated (508)	System time has been updated
TEST	test (506)	test event
USB	usb-eth-added (903)	USB Ethernet device has been added
	usb-eth-removed (904)	USB Ethernet device has been removed
	usb-serial-added (905)	USB serial device has been added
	usb-serial-removed (906)	USB serial device has been removed
	usb-storage-added (901)	USB storage device has been added
	usb-storage-removed (902)	USB storage device has been removed
WAN	wan-down (101)	WAN link went down
	wan-up (102)	WAN link came up

7.6.8. SMS

This page lets you turn on the SMS event notification service and enable remote control via SMS.

Administration

On RACOM routers it is possible to receive or send short messages (SMS) over each mounted modem (depending on the assembly options). Messages are received by querying the SIM card over a modem, so prior to that, the required assignment of a SIM card to a modem needs to be specified on the SIMs page.

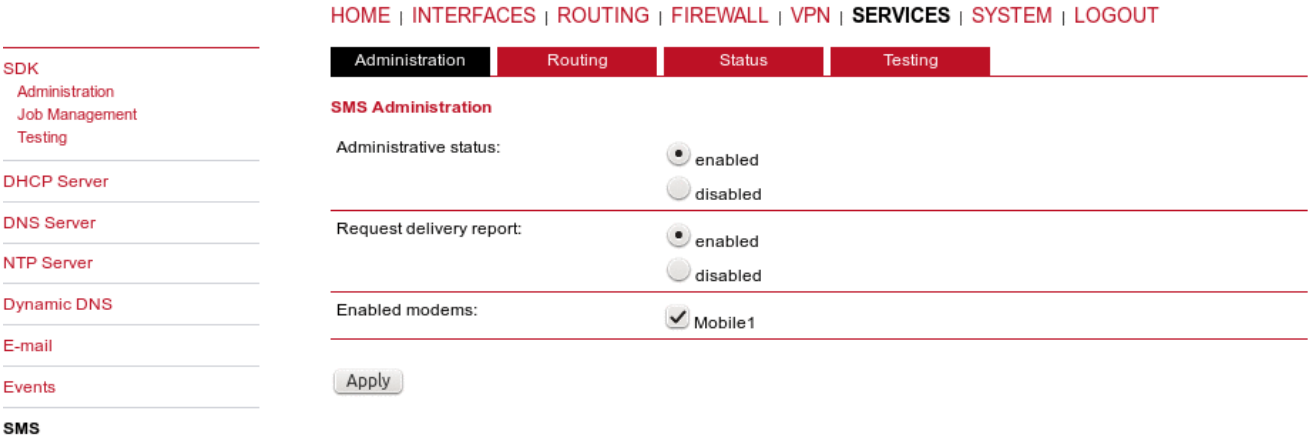
Please bear in mind, in case you are running multiple WWAN interfaces sharing the same SIM, that the system may switch SIMs during operation which will also result in different settings for SMS communication.

Received messages are pulled from the SIMs and temporarily stored on the router but get cleared after a system reboot. Please consider to consult an SDK script in case you want to process or copy them.

Sending messages heavily depends on the registration state of the modem and whether the provided SMS Center service works and may fail. You may use the sms-report-received event to figure out whether a message has been successfully sent.

Please do not forget that modems might register roaming to foreign networks where other fees may apply. You can manually assign a fixed network (by LAI) in the SIMs section.

The relevant page can be used to enable the SMS service and specify on which modem should operate.

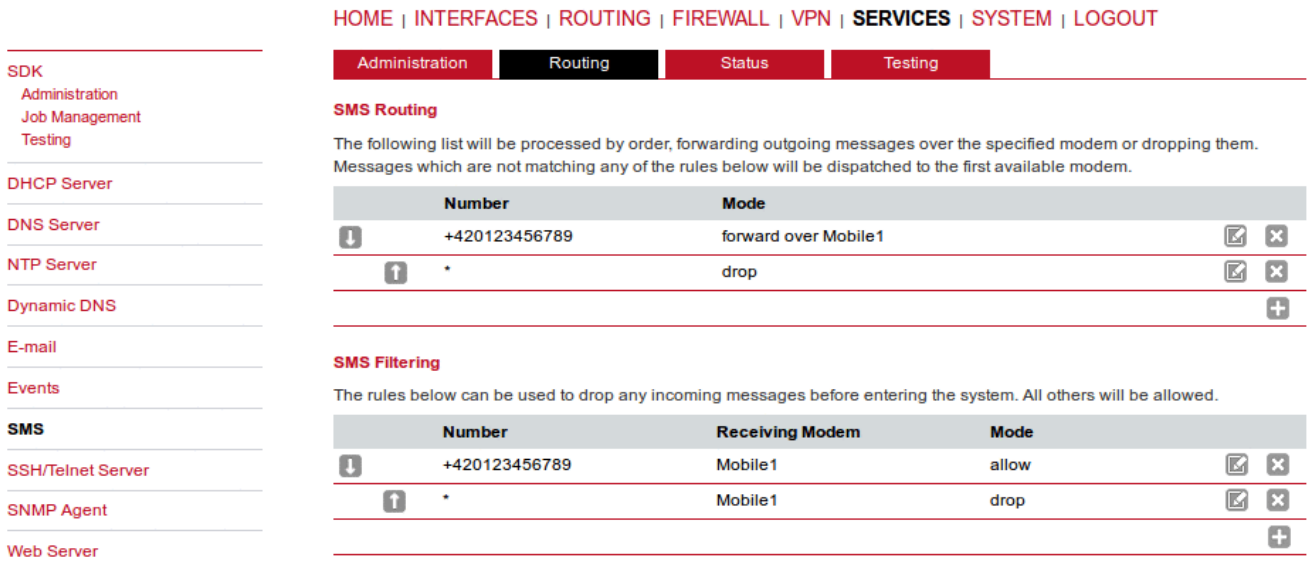


Administrative status: Enable or disable SMS notifications and control

Request delivery report: Enable or disable receiving the confirmation whether SMS was successfully received or not. This can be then read in the SMS Status menu.

Routing & Filtering

By using SMS routing you can specify outbound rules which will be applied whenever messages are sent. You can forward them to an enabled modem. For a particular number, you can for instance enforce messages be sent over a dedicated SIM.



Phone numbers can also be specified by regular expressions, here are some examples:

```
+12345678    Specifies a fixed number
+1*          Specifies any numbers starting with +1
+1*9         Specifies any numbers starting with +1 and ending with 9
+[12]*       Specifies any numbers starting with either +1 or 2
```

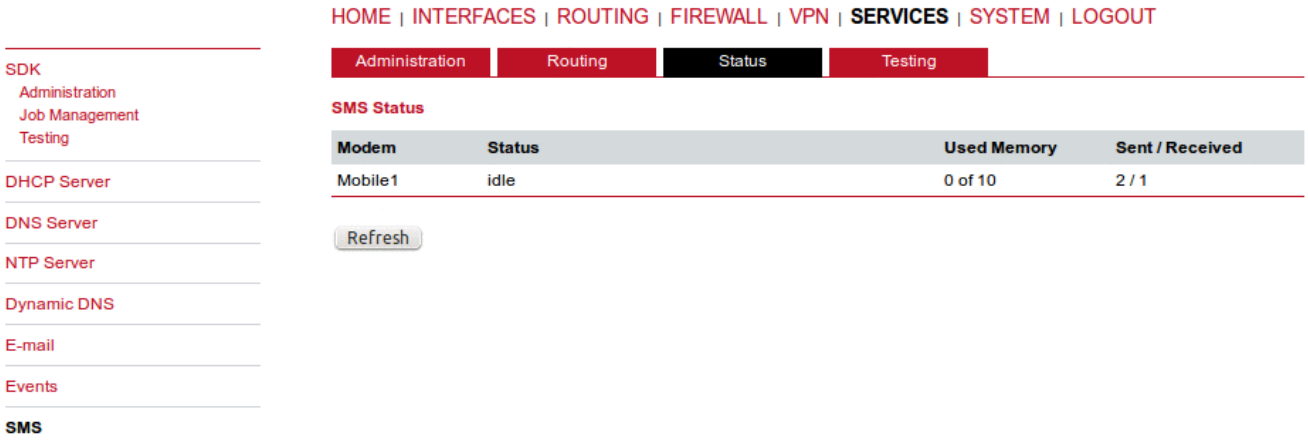
Please note that numbers have to be entered in international format including a valid prefix. On the other hand, you can also define rules to drop outgoing messages, for instance, when you want to avoid using any expensive service or international numbers.

Both types of rules form a list will be processed in order, forwarding outgoing messages over the specified modem or dropping them. Messages which are not matching any of the rules below will be dispatched to the first available modem.

Filtering serves a concept of firewalling incoming messages, thus either dropping or allowing them on a per-modem basis. The created rules are processed in order and in case of matches will either drop or forward the incoming message before entering the system. All non-matching messages will be allowed.

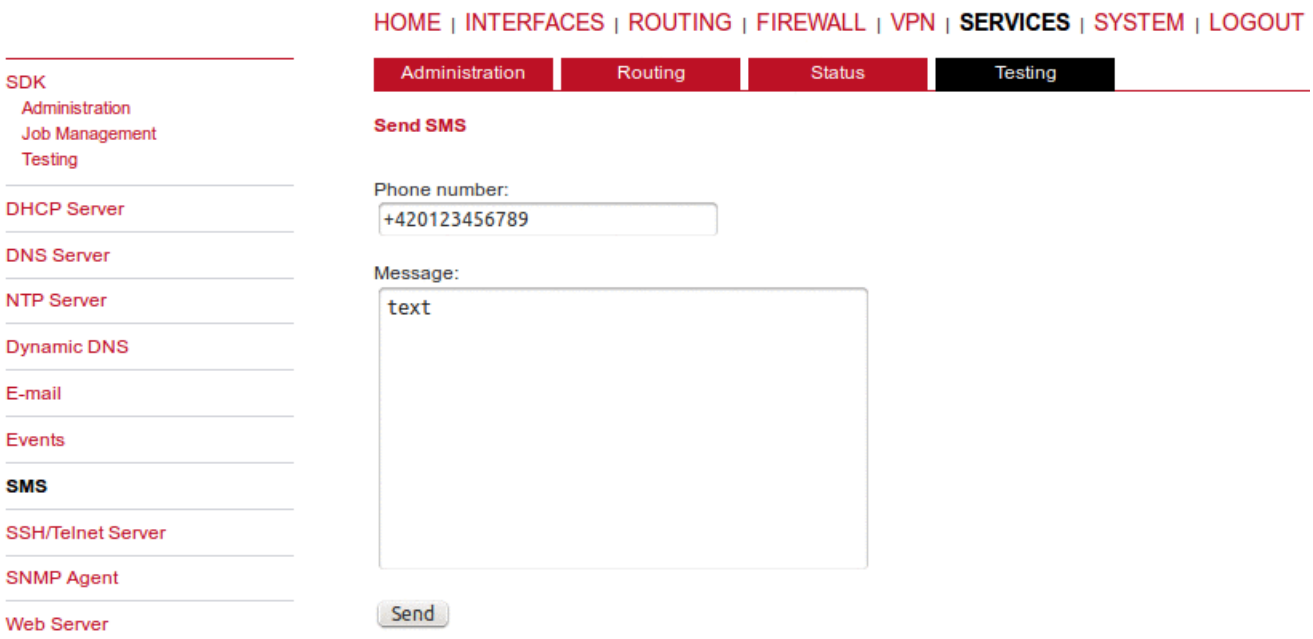
Status

The status page can be used to the current modem status and get information about any sent or received messages. There is a small SMS inbox reader which can be used to view or delete the messages. Please note that the inbox will be cleared each midnight in case it exceeds 512 kbytes of flash usage.



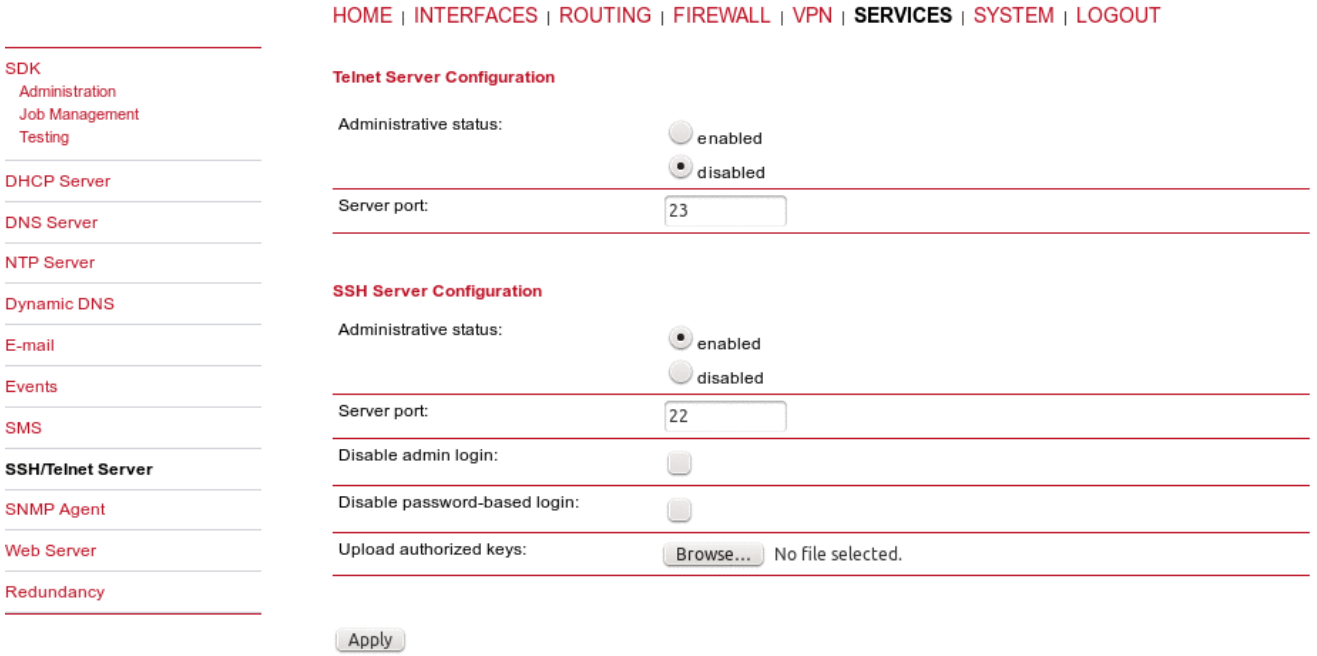
Testing

This page can be used to test whether SMS sending in general or filtering/routing rules works. The maximum length per message part is limited to 160 characters, we also suggest to exclusively use characters which are supported by the GSM 7-bit alphabet.



7.6.9. SSH/Telnet Server

Apart from the Web Manager, the SSH and Telnet services can be used to log into the system. Valid users include root and admin as well as additional users as they can be created in the User Accounts section. Please note, that a regular system shell will only be provided for the root user, the CLI will be launched for any other user whereas normal users will only be able to view status values, the admin user will obtain privileges to modify the system.



Please note that these services will be accessible from the WAN interface also. In doubt, please consider to disable or restrict access to them by applying applicable firewall rules.

The following parameters can be applied to the Telnet service:

Administrative status: Whether the Telnet service is enabled or disabled

Server port: The TCP port of the service (usually 23)

The following parameters can be applied to the SSH service:

Administrative status: Whether the SSH service is enabled or disabled

Server port: The TCP port of the service (usually 22)

Disable admin login: If checked, access via SSH for admin and root users will be blocked. Other users may have access as usual, but with restricted privileges.

Disable password-based login: By turning on this option, all users will have to authenticate by SSH keys which can be uploaded to the router.

7.6.10. SNMP Agent

M!DGE/MG102i is equipped with an SNMP daemon, supporting basic MIB tables (such as ifTable), plus additional enterprise MIBs to manage multiple systems. M!DGE/MG102i OID starts with 1.3.6.1.4.1.33555.10 prefix. The corresponding VENDOR MIB can be downloaded from the router.

M!DGE/MG102i extensions contain support for:

- Rebooting the device
- Updating to a new system software via FTP/TFTP/HTTP
- Updating to a new system configuration via FTP/TFTP/HTTP
- Getting WWAN/GNSS/WLAN/DIO information

Note

Attention must be paid to the fact that SNMP passwords have to be more than 8 characters long. Shorter passwords will be doubled for SNMP, e.g. 'admin01' becomes 'admin01admin01'.

SNMP extensions can be read and triggered as follows:

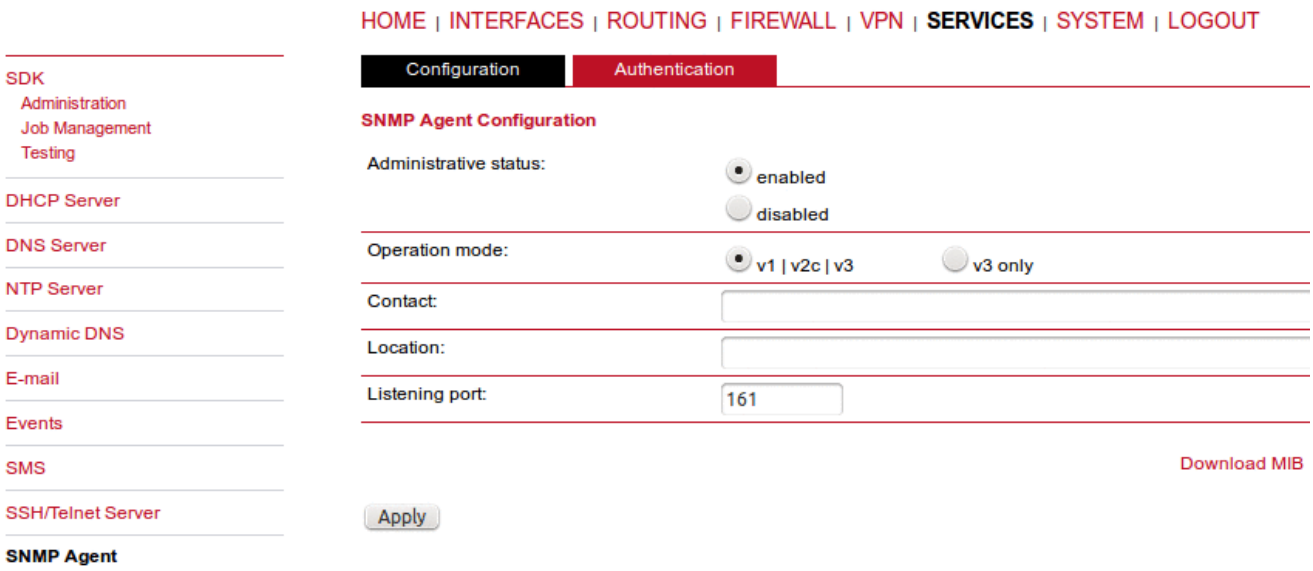
- To get system software version:
  snmpget -v 3 -u admin -n "" -l authNoPriv -a MD5 -x DES -A admin01admin01 192.168.1.1 1.3.6.1.4.1.33555.10.40.1.0
- To get a kernel version:
  snmpget -v 3 -u admin -n "" -l authNoPriv -a MD5 -x DES -A admin01admin01 192.168.1.1 1.3.6.1.4.1.33555.10.40.2.0
- To get a serial number:
  snmpget -v 3 -u admin -n "" -l authNoPriv -a MD5 -x DES -A admin01admin01 192.168.1.1 1.3.6.1.4.1.33555.10.40.3.0
- To restart the device:
  snmpset -v 3 -u admin -n "" -l authNoPriv -a MD5 -x DES -A admin01admin01 192.168.1.1 1.3.6.1.4.1.33555.10.40.10.0 i 1
- To run a configuration update:
  snmpset -v 3 -u admin -n "" -l authNoPriv -a MD5 -x DES -A admin01admin01 192.168.1.1 1.3.6.1.4.1.33555.10.40.11.0 s "http://server/directory"

Note

config Update expects a zip-file named <serial-number>.zip in the specified directory which contains at least a "user-config.zip".
Supported protocols are TFTP, HTTP(s) and FTP.
Specifying a username/password or port is not yet supported.

- get configuration update status:
  snmpget -v 3 -u admin -n "" -l authNoPriv -a MD5 -x DES -A admin01admin01 192.168.1.1 1.3.6.1.4.1.33555.10.40.12.0
  The return value can be one of: (1) succeeded, (2) failed, (3) inprogress, (4) notstarted.
- run software update:
  snmpset -v 3 -u admin -n "" -l authNoPriv -a MD5 -x DES -A admin01admin01 192.168.1.1 1.3.6.1.4.1.33555.10.40.13.0 s "http://server/directory"
- get software update status:
  snmpget -v 3 -u admin -n "" -l authNoPriv -a MD5 -x DES -A admin01admin01 192.168.1.1 1.3.6.1.4.1.33555.10.40.14.0
  Return value can be either of: (1) succeeded, (2) failed, (3) inprogress, (4) notstarted.

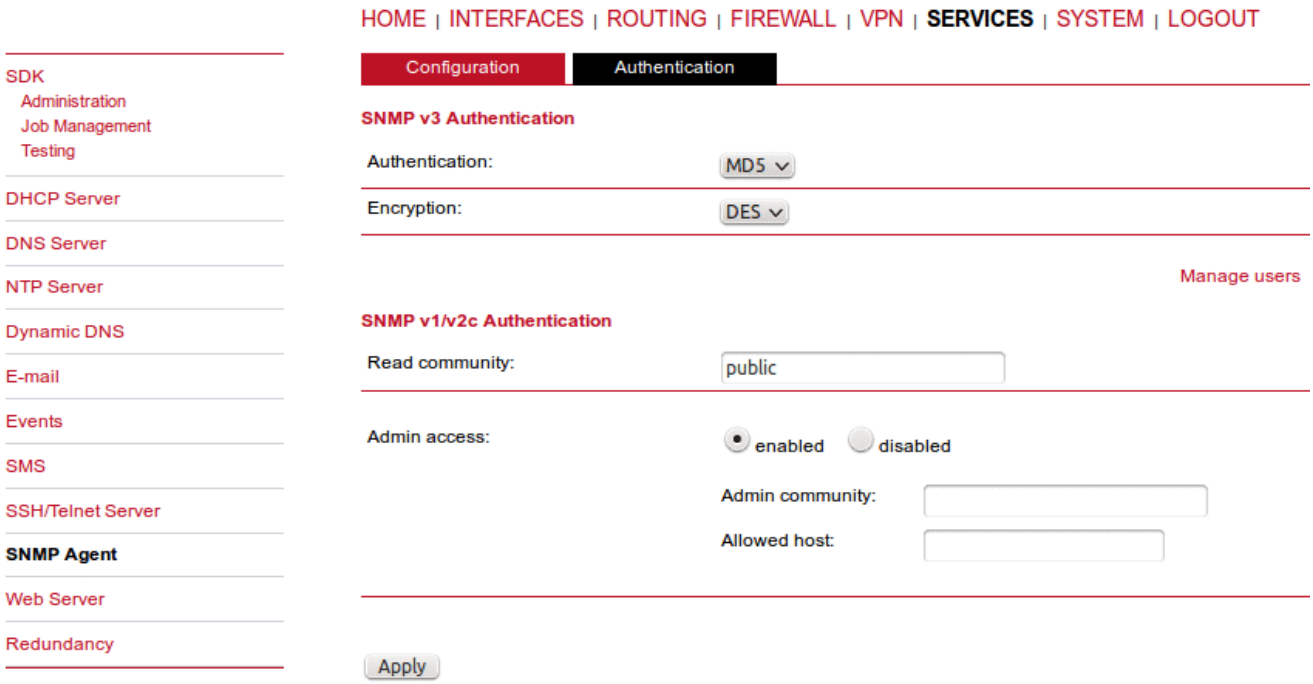
SNMP Configuration



Administrative status:	Enable or disable the SNMP agent
Operation mode:	Specifies if agent should run in compatibilty mode or for SNMPv3 only
Contact:	System maintainer or other contact information
Location:	Device location
Listening port	SNMP agent port

Once the SNMP agent is enabled, SNMP traps can be generated using SDK scripts or can be triggered by various Events (see the SYSTEM → Events menu).

SNMP Authentication



When running in SNMPv3, it is possible to configure the following authentication settings:

Authentication: Defines the authentication (MD5 or SHA)

Encryption: Defines the privacy protocols to use (DES or AES)

In general, the admin user can read and write any values. Read access will be granted to any other system users.

There is no authentication/encryption in SNMPv1/v2c and should not be used to set any values. However, it is possible to define its communities and authoritive host which will be granted administrative access.

Read community: Defines the community name for read access

Admin community: Defines the community name for admin access

Allowed host: Defines the host which is allowed for admin access

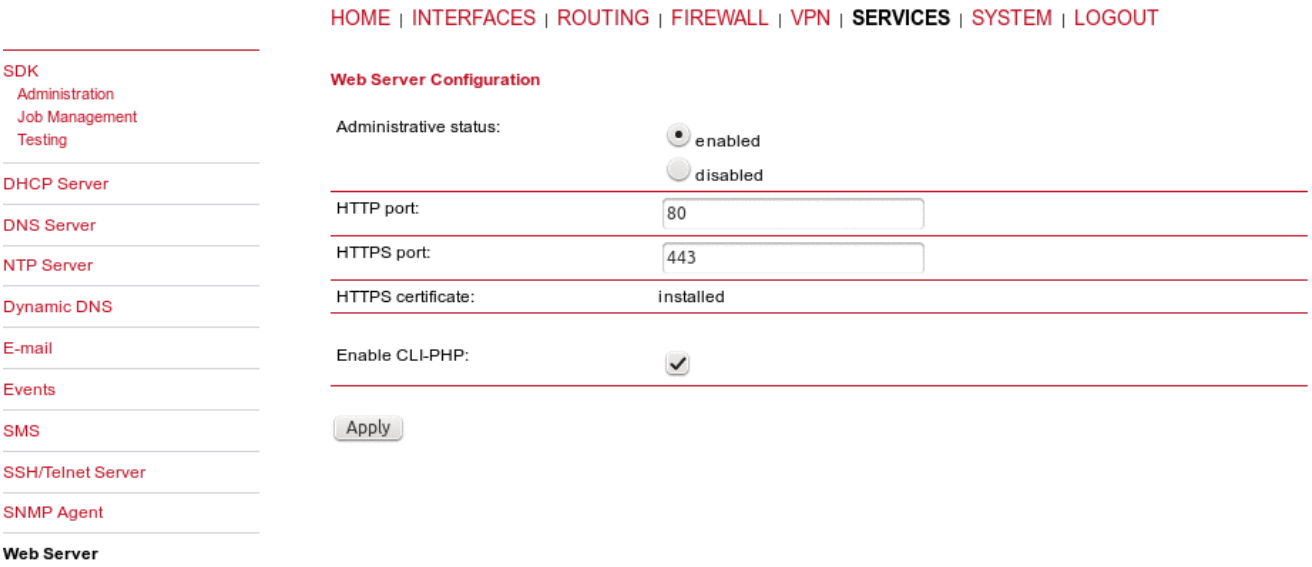
Note

The SNMP daemon is also listening on WAN interfaces and it is therefore suggested to restrict the access via the firewall.

7.6.11. Web Server

This page can be used to configure different ports for accessing the Web Manager via HTTP/HTTPS. We strongly recommend to use HTTPS when accessing the web service via a WAN interface as the communication will be encrypted and thus avoids any misuse of the system.

In order to enable HTTPS you would need to generate or upload a server certificate in the section SYSTEM-Keys and Certificates.



Administrative status:	Enable or disable the Web server
HTTP port:	Web server port for HTTP connections
HTTPS port:	Web server port for HTTPS connections
HTTPS certificate:	Either information that the certificate is 'installed' or a link to create such certificate.
Enable CLI-PHP:	Enable CLI-PHP service (see Section 8.16, “CLI–PHP”)

7.6.12. Redundancy

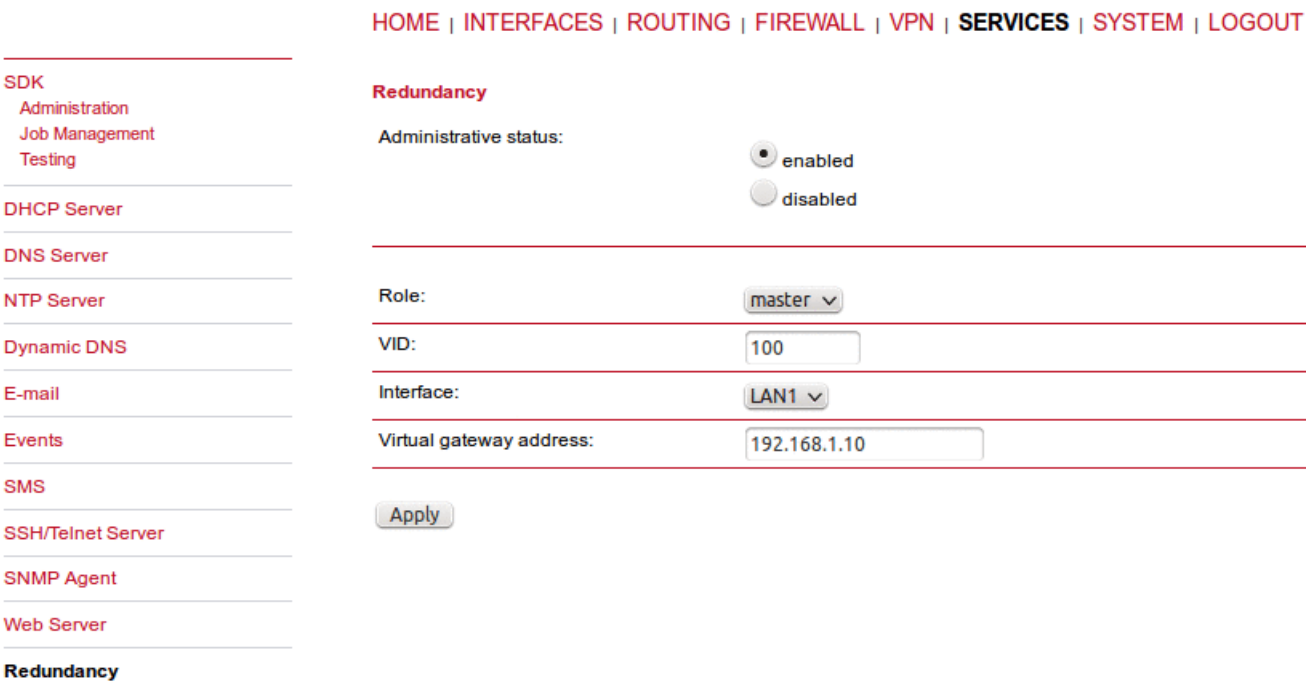
This section can be used to set up a redundant pair of M!DGE/MG102is (or other systems) by running the Virtual Router Redundancy Protocol (VRRP) among them. A typical VRRP scenario defines the first host playing the master and another the backup device, they both define a virtual gateway IP address which will be distributed by gratuitous ARP messages for updating the ARP cache of all LAN hosts and thus redirecting the packets accordingly.

A takeover will happen within approximately 3 seconds as soon as the partner is no longer reachable (checked via multicast packets). This may happen when one device is rebooting or the Ethernet link went down. Same applies when the WAN link goes down.

In case DHCP has been activated, please keep in mind that you will need to reconfigure the DHCP gateway address offered by the server and let them point to the virtual gateway address. In order to avoid conflicts you may turn off DHCP on the backup device or even better, split the DHCP lease range in order to prevent any lease duplication.

Note

M!DGE/MG102i assigns a priority of 100 to the master and 1 to the backup router. Please adapt the priority of your third-party device appropriately.

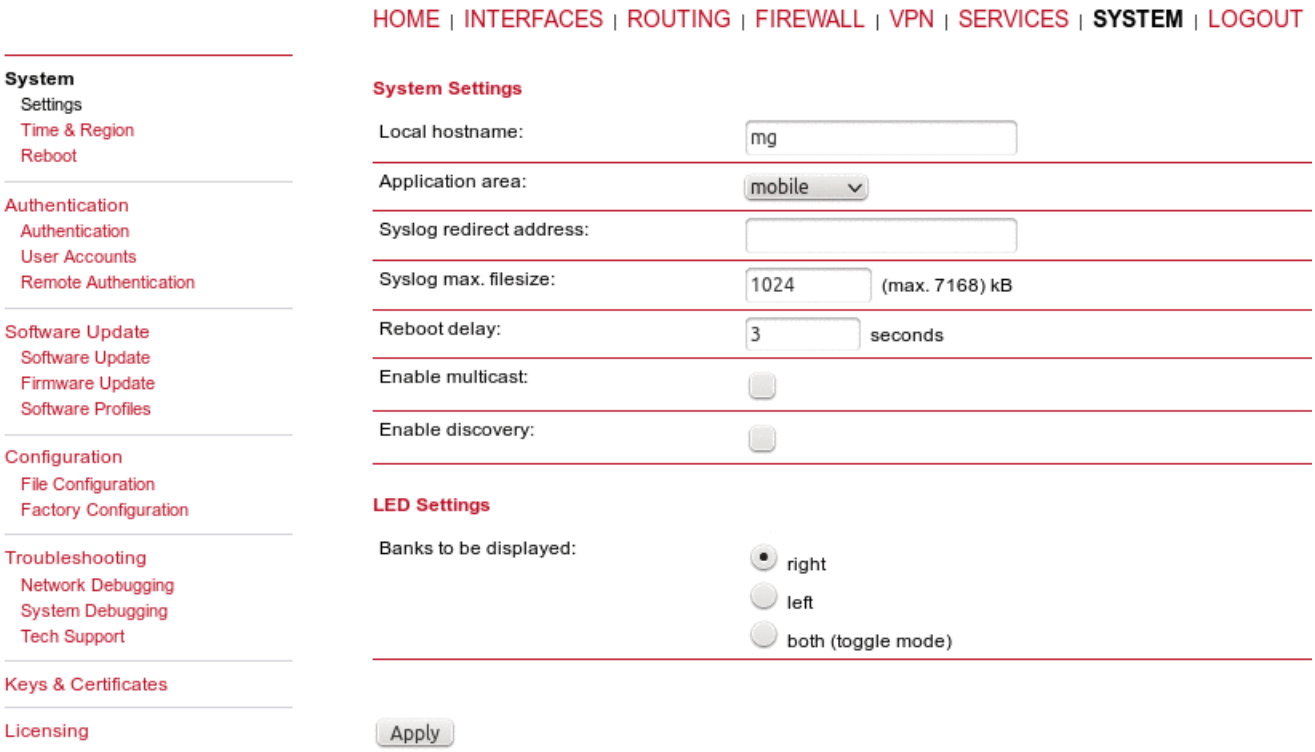


Administrative status:	Enable or disable Redundancy
Role:	Role of this system (either master or backup)
VID:	The Virtual Router ID (you can theoretically run multiple instances)
Interface:	Interface on which VRRP should be performed
Virtual gateway address:	Virtual gateway address formed by the participating hosts

7.7. SYSTEM

7.7.1. System

Settings

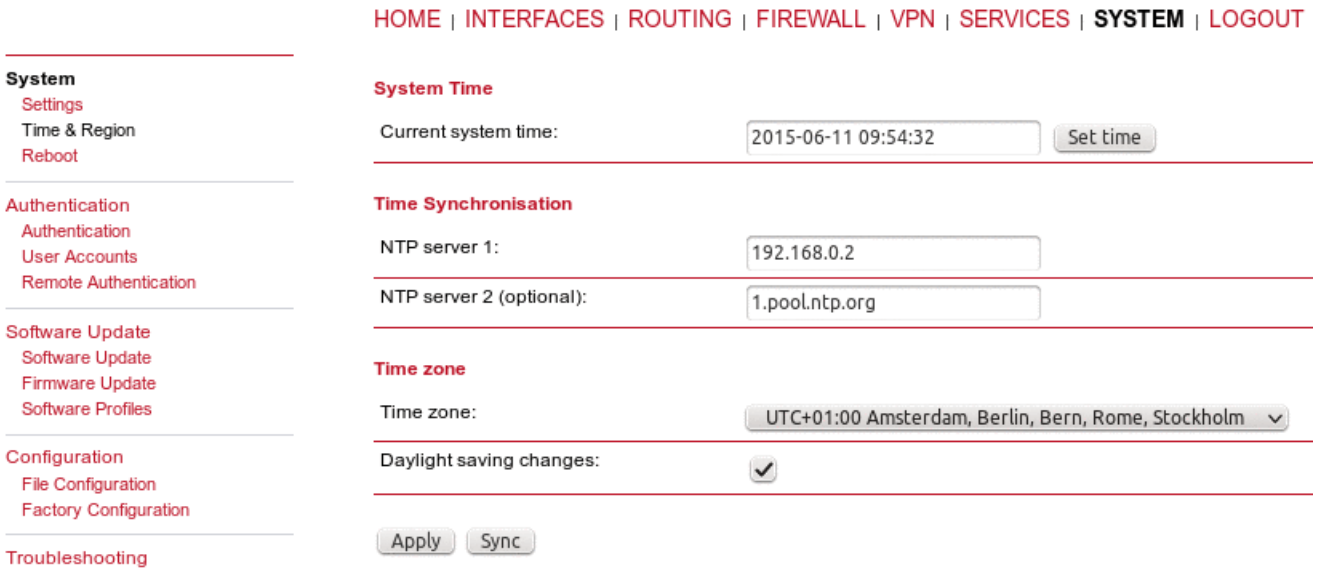


Local host name:	The local system hostname
Application area:	The desired application area which influences the system behaviour such as registration timeouts when operating in the mobile environment.
Syslog redirect address:	The host where system log messages should be forwarded to. You can use for example a tiny system log server for Windows included in TFTP32.
Syslog max. file size:	The maximum log file size in kilobytes until it's rotated
Reboot delay:	The number of seconds to wait before the reboot is initiated (might be needed for some system-rebooting events)
Enable multicast	Activates an IGMP proxy and enables multicast routing for the current hotlink interface towards LAN interfaces.
Enable discovery	Enables host discovery over LLDP or CDP. Discovered neighbours can be found on the LAN status page or via SNMP.
LED Settings:	You can configure the behaviour of the status LEDs on the front panel of your device. They are usually divided into two banks - left (M!DGE) or upper (MG102i) for the digital IO port status or right (M!DGE) or lower (MG102i) for the connection status indication.

You may configure toggle mode, so that the LEDs periodically show both bank states. See the LEDs description in Section 4.3, “Indication LEDs”.

Time & Region

Network Time Protocol (NTP) is a protocol for synchronizing the clocks of computer systems over packet-switched, variable-latency data networks. M!DGE/MG102i can synchronize its system time with an NTP server. If enabled, time synchronisation is usually triggered after a WAN link has come up but before starting any VPN connections. Further time synchronisations are scheduled in the background every 60 minutes.



Current system time: The current system time which can be synchronized agains a valid NTP server or set manually. If manually set, the time is lost after the reboot.

NTP server 1: The primary NTP server IP address or hostname

NTP server 2 (optional): The optional secondary NTP server IP address or hostname

Time zone: Time zone based on your geographical location

Daylight saving changes: This option can be used to reflect daylight saving changes (e.g. switching from summer to standard time) depending on the selected time zone.

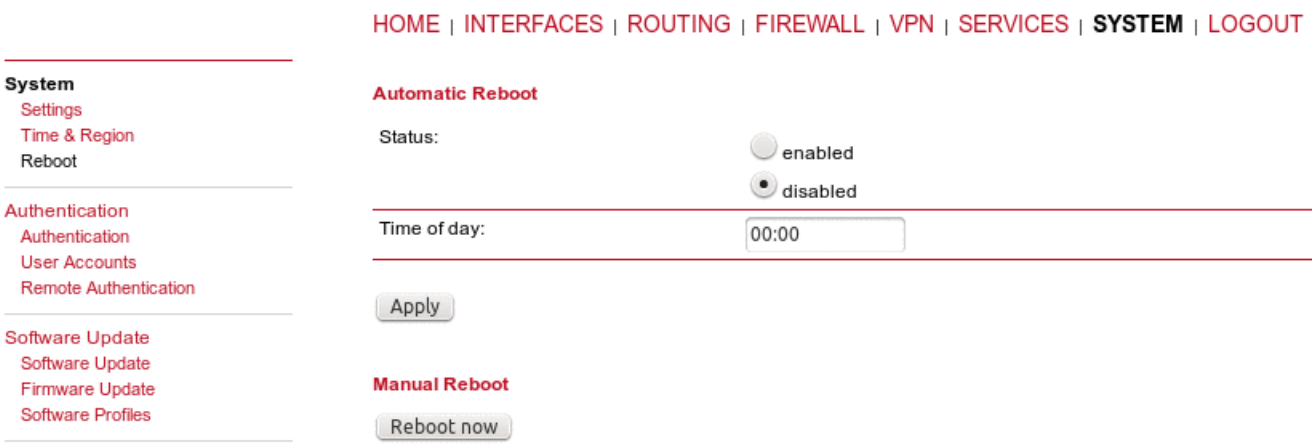
Sync will perform the time synchronisation immediatelly.

Note

The System information menu has been moved into the HOME menu (since firmware 3.7.x).

Reboot

This menu can be used to reboot the system. All WAN links will be interrupted.



7.7.2. Authentication

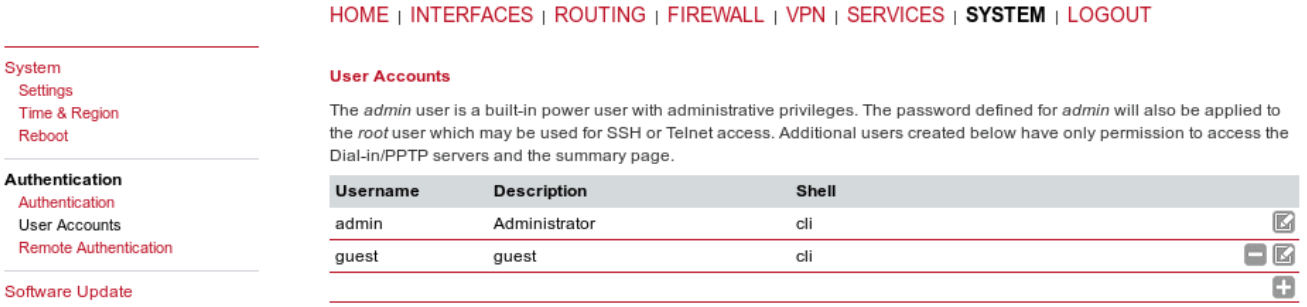
Authentication

This page offers a simple shortcut to allow only secure connections (SSH, HTTPS) for managing the router. If the option "Secure authentication preferred" is set, users will be redirected to HTTPS but can still login via HTTP/telnet.

User Accounts

This page lets you manage the user accounts on the device.

The standard admin user is a built-in power user that has permission to access the Web Manager and other administrative services and is used by several services as the default user. Keep in mind that the admin password will be also applied to the root user which is able to enter a system shell. Any other user represents a user with lower privileges, for instance it has only permission to view the status page or retrieve status values when using the CLI.


HOME | INTERFACES | ROUTING | FIREWALL | VPN | SERVICES | SYSTEM | LOGOUT
System
Settings
Time & Region
Reboot
Authentication
Authentication
User Accounts
Remote Authentication
Software Update
User Accounts
The admin user is a built-in power user with administrative privileges. The password defined for admin will also be applied to the root user which may be used for SSH or Telnet access. Additional users created below have only permission to access the Dial-in/PPTP servers and the summary page.
Username
Description
Shell
admin
Administrator
cli
guest
guest
cli

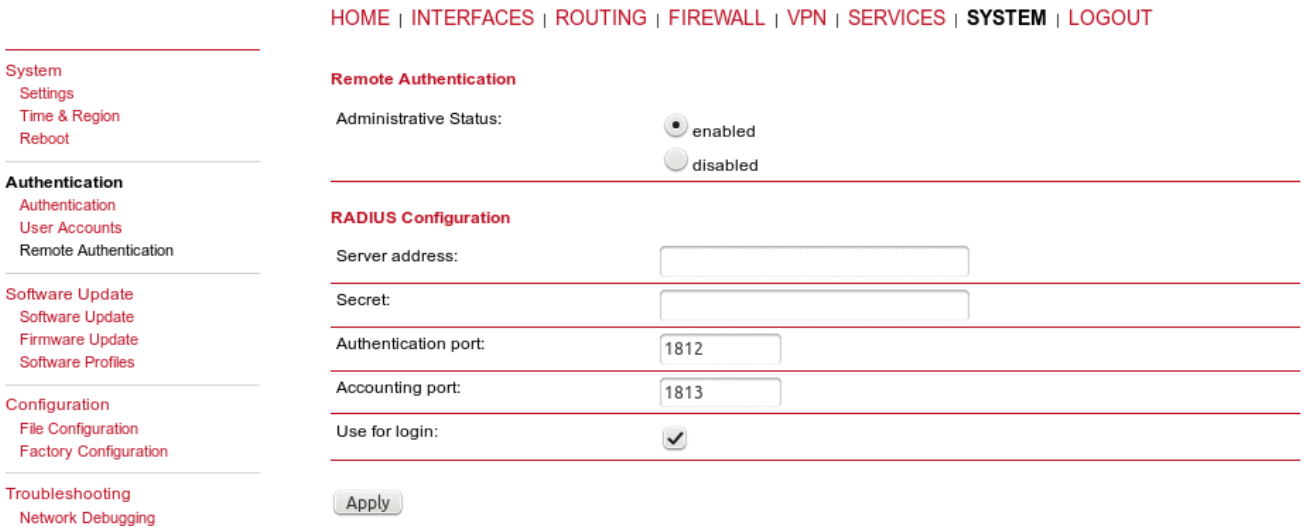
Username: Define a user name

Description: The user description

Shell	Choose whether the CLI or shell command prompt shall be started after the user is logged in via SSH/Telnet. This is currently applicable only for the admin user.
Password:	Define a password
Password confirmation:	Confirm the password

Remote Authentication

A remote RADIUS server can be used to authenticate users. This applies for the Web Manager and other services supporting and incorporating remote authentication.

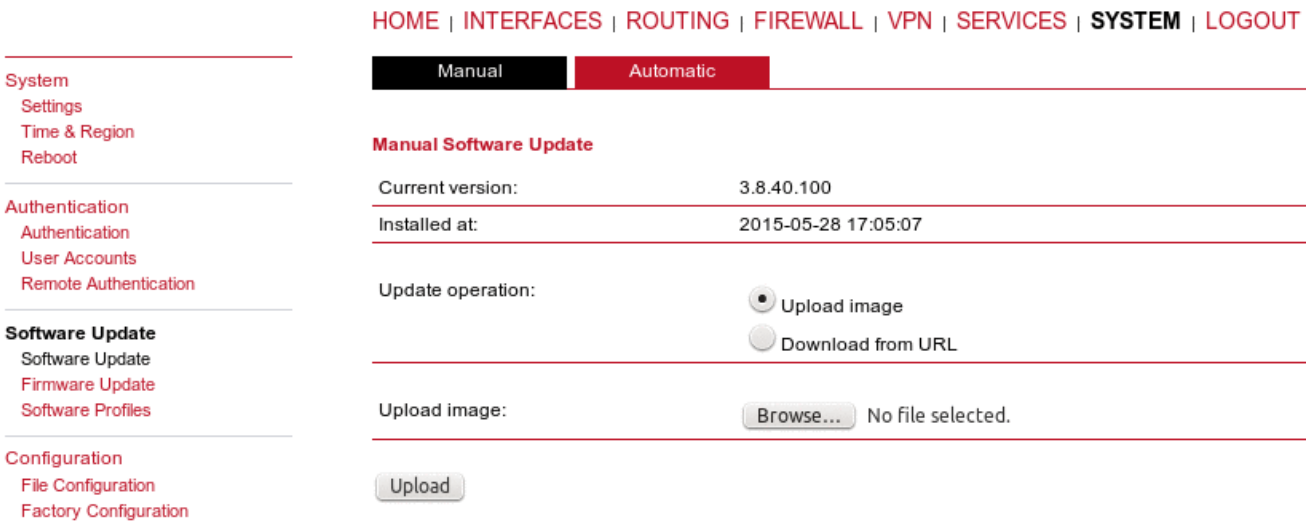


Administrative status:	Enable or disable remote authentication
Server address:	RADIUS server address
Secret:	Secret used to authenticate against the RADIUS server
Authentication port:	Port used for authentication
Accounting port:	Port used for accounting messages
Use for login:	This option enables remotely-defined users to access the Web Manager

7.7.3. Software Update

Manual Software Update

This menu can be used to run a manual software update.



Update operation: The update operation method being used. You can upload the image or download it from the given URL

URL: You can upload the image or download it from the given URL.

When issuing a software update, the current configuration (including files like keys/certificates) will be backuped. Any other modifications to the filesystem will be erased. The configuration is generally backward-compatible. We also apply forward compatibility when downgrading to a previous software within the same release line (e.g. 3.6.40.X), which is accomplished by sorting out unknown configuration directives which actually may lead to loss of settings and features. Therefore, it's always a good idea to keep a copy of the working configuration. Generally, we do not recommend downgrading the software.

Important

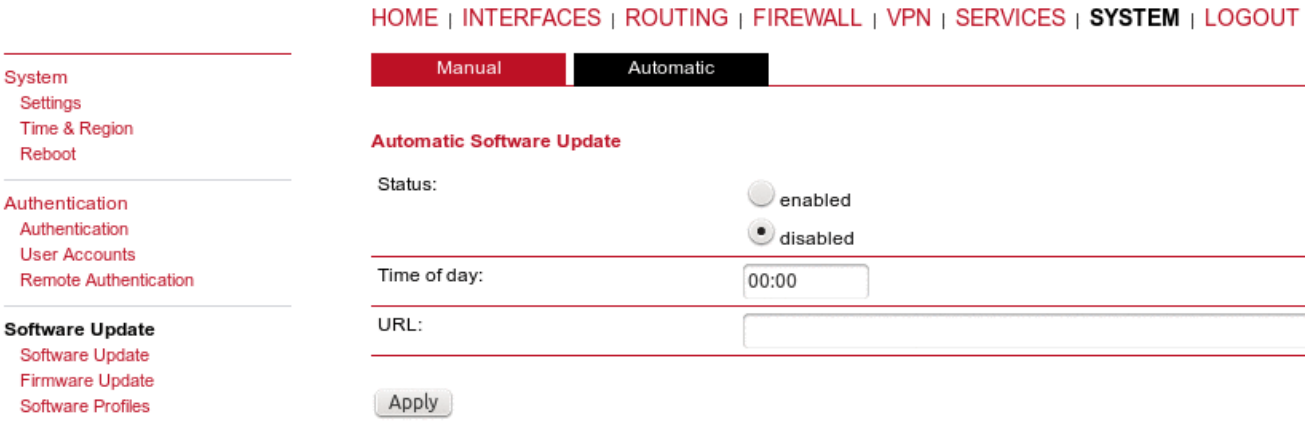
In case you perform a major downgrade to a previous release line (e.g. 3.6.40.X to 3.5.40.X), the configuration will be set to factory defaults. Also keep in mind, that some hardware features may not work (e.g. if not implemented in that version). In doubt, please consult our support team.

A software image can be either uploaded via the Web Manager or retrieved from a specific URL. It will be unpacked and deployed to a spare partition which gets activated if the update completed successfully. The whole procedure is accompanied by all green LEDs flashing up, the subsequent system reboot gets denoted by a slowly blinking Status LED. The backuped configuration will be applied at bootup and the Status LED will blink faster during this operation. Depending on your configuration, this may take a while.

Important

The upgrade from 3.6.41.x and newer firmwares is fully compatible. If you upgrade from older releases, you have to reset the unit into the factory settings (only if you need to use the serial interface Protocol server functionality). The previously saved configuration can be uploaded to the station manually afterwards.

Automatic Software Update

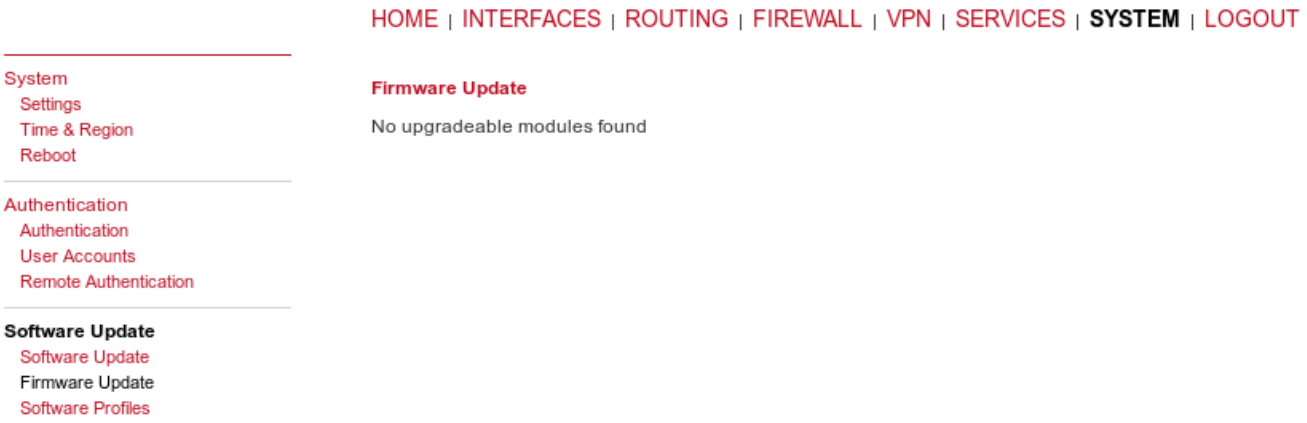


Status: Enable/disable automatic software update

Time of day: Every day at this time M!DGE/MG102i will do a check for updates

URL: The server URL where the software update package should be downloaded from. Supported protocols are TFTP, HTTP(s), and FTP

Firmware Update



This menu can be used to perform a firmware update of a specific module.

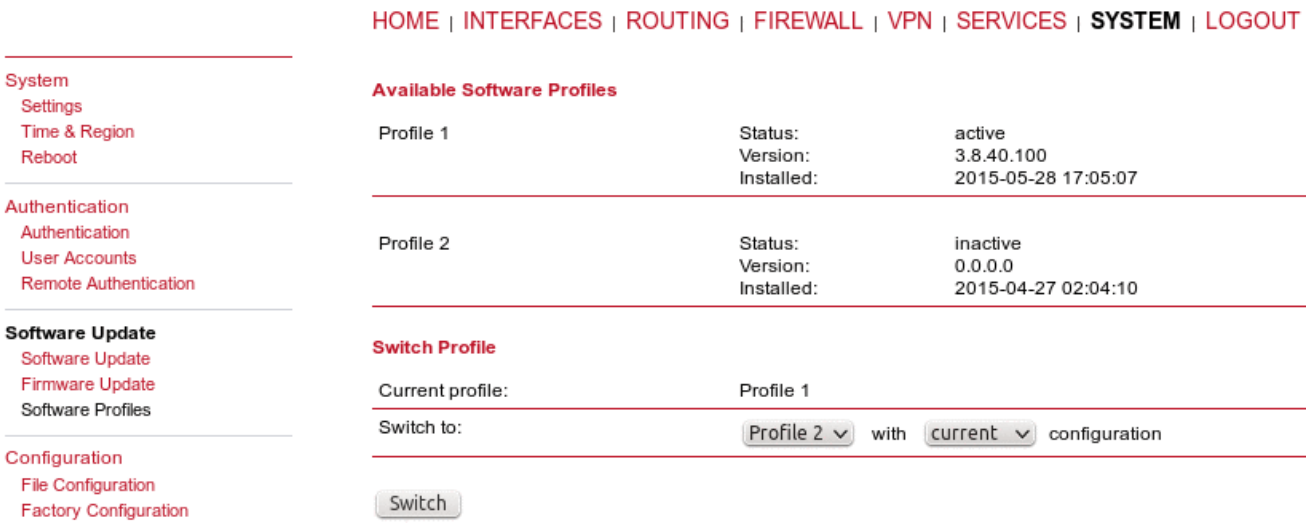
Update operation: The update operation method being used. You can upload a firmware package or download the files from a specifc URL.

URL: The server URL where the firmware files should be downloaded from. Supported protocols are TFTP, HTTP, HTTPS, and FTP (protocol://server/path/file).

Software Profiles

In every router you have two software profiles. One is active (currently used) and one is inactive. You can easily switch between these profiles any time.

It can be for example useful when there is some issue with the newest firmware and you need to restore the previous firmware version easily. Or you can just test some new features in the newest firmware and then get back to the previous one.



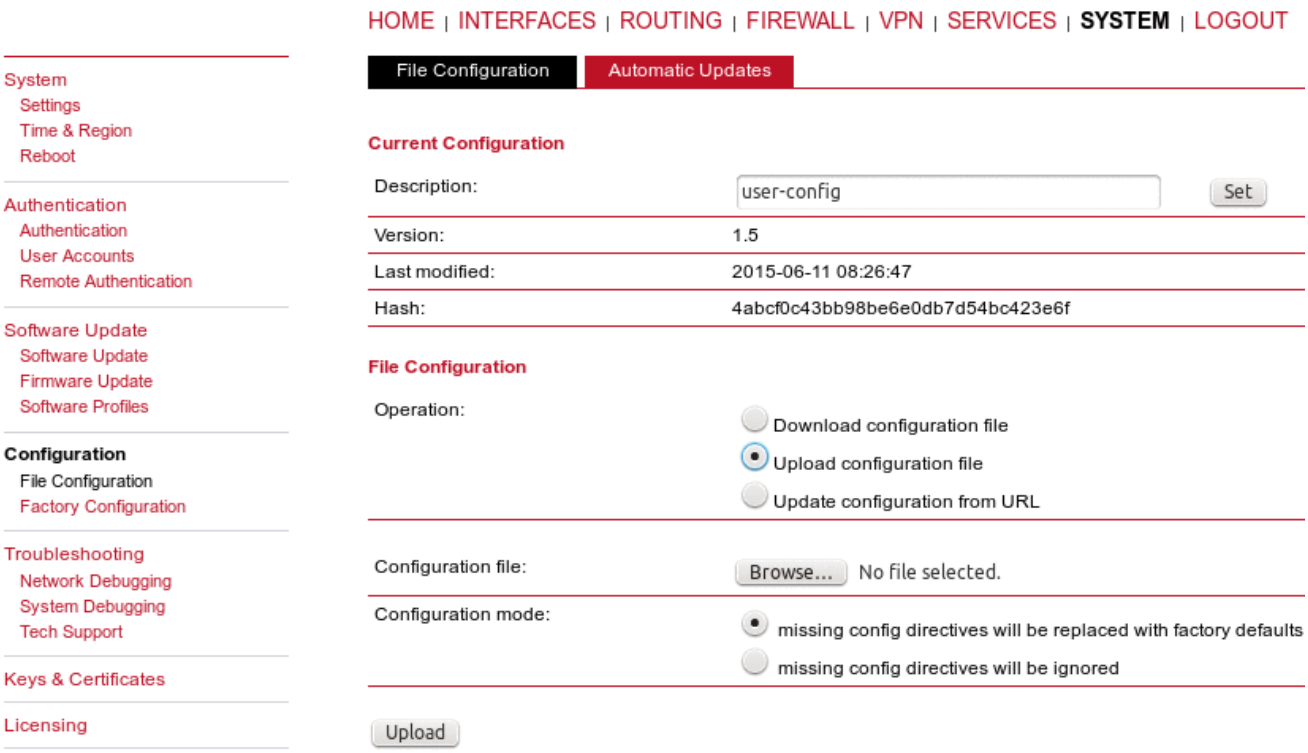
7.7.4. Configuration

Configuration via the Web Manager becomes tedious for large volumes of devices. M!DGE/MG102i therefore offers automatic and manual file-based configuration to automate things. Once you have successfully set up the system you can back up the configuration and restore the system with it afterwards. You can either upload a single configuration file (.cfg) or a complete package (.zip) containing the configuration file and a packed version of other essential files (such as certificates).

File Configuration

This section can be used to download the currently running system configuration (including essential files such as certificates).

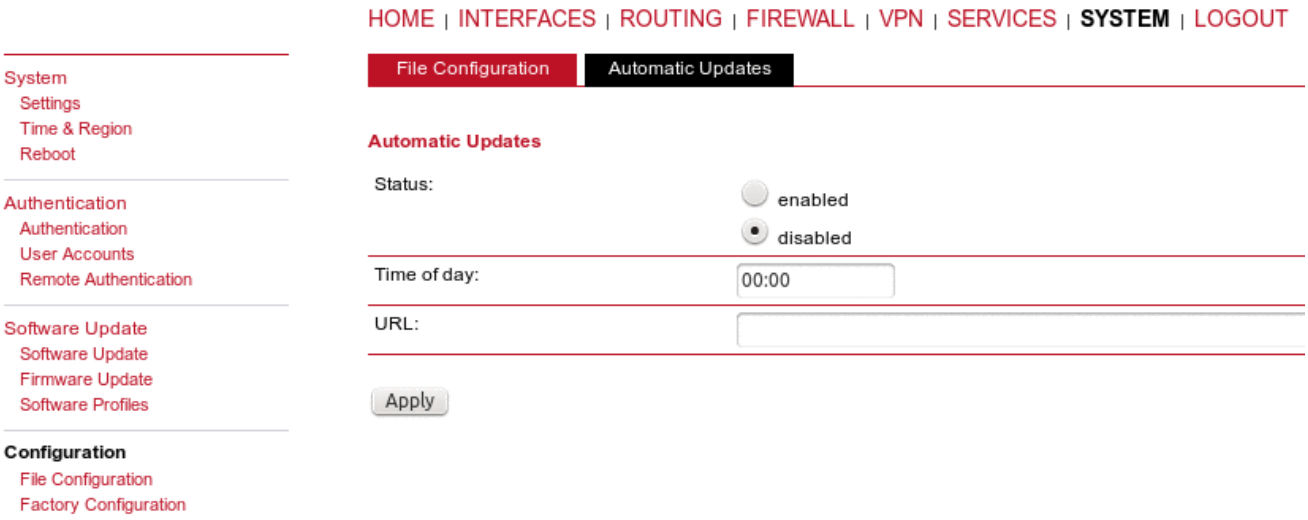
The current configuration file is updated after every change and the time of this update is displayed along with a configuration version and a security hash. The current configuration can be updated manually by pressing the Apply button.



In order to restore a particular configuration you can upload a configuration previously downloaded or update configuration from the provided URL link.

You can choose between missing configuration directives stay the same as in the currently running configuration.

Automatic Updates



Status: Enable/disable automatic configuration update

Time of day: Time of day when the system will check for updates

URL: The server URL where the configuration file should be retrieved from (supported protocols are HTTP(s), TFTP, FTP)

Factory Configuration

This menu can be used to reset the device to factory defaults. Your current configuration will be lost.

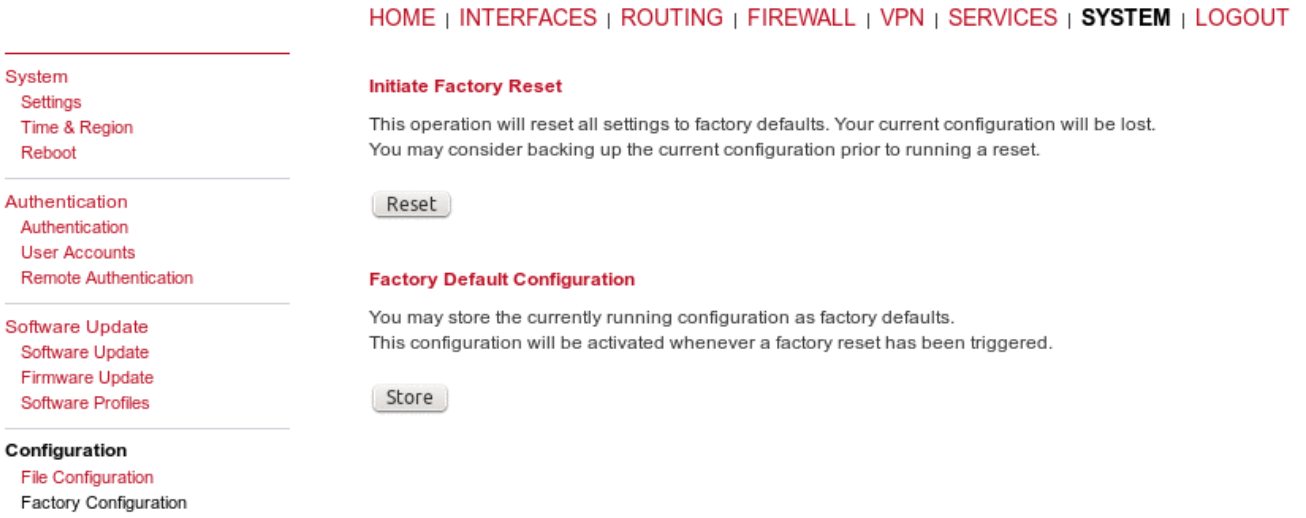
This procedure can also be initiated by pressing and holding the Reset button for at least 10 seconds. A successfully initiated factory reset can be noticed by all LEDs being turned on.

Factory reset will set the IP address of the first Ethernet interface back to 192.168.1.1. You will be able to communicate again with the device using the default network parameters.

You may store the currently running configuration as factory defaults which will reside active even when a factory reset has been initiated (e.g. by your service staff). Please ensure that this corresponds to a working configuration. A real factory reset to the default settings can be achieved by restoring the original factory configuration and initiating the factory reset again.

Important

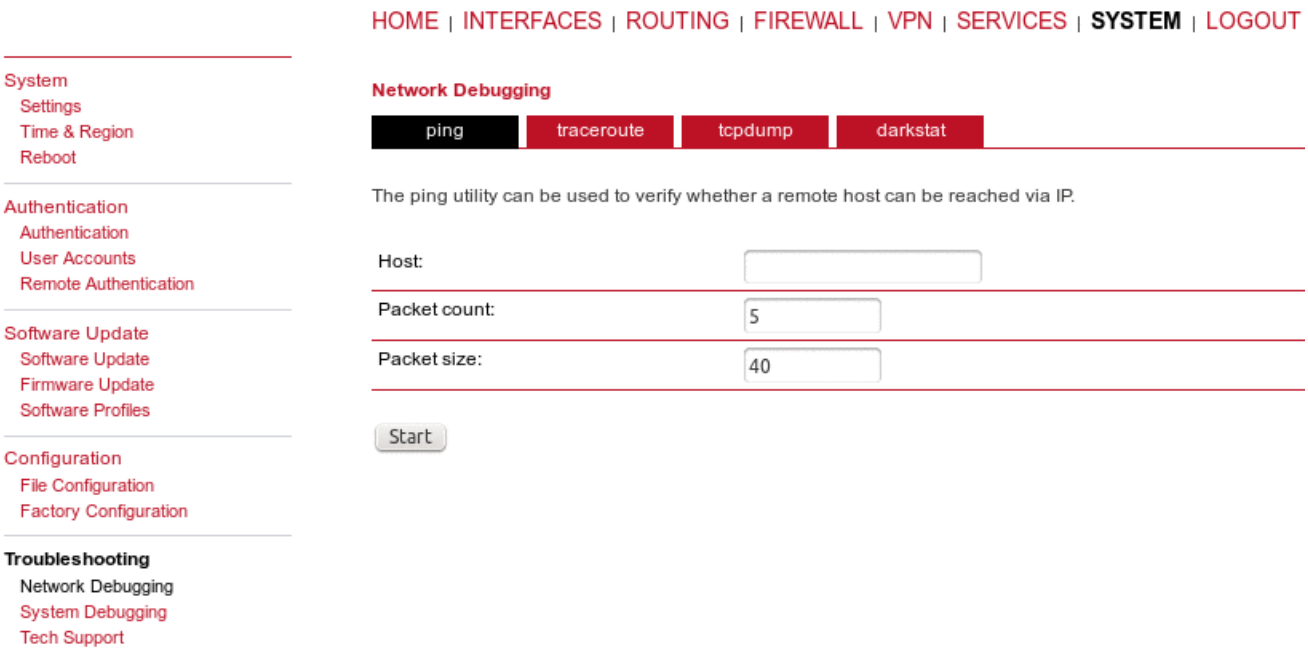
If you store the currently running configuration as the factory defaults, have in mind that the password is also stored within this configuration.


HOME | INTERFACES | ROUTING | FIREWALL | VPN | SERVICES | SYSTEM | LOGOUT
System
Settings
Time & Region
Reboot
Authentication
Authentication
User Accounts
Remote Authentication
Software Update
Software Update
Firmware Update
Software Profiles
Configuration
File Configuration
Factory Configuration
Initiate Factory Reset
This operation will reset all settings to factory defaults. Your current configuration will be lost.
You may consider backing up the current configuration prior to running a reset.
Reset
Factory Default Configuration
You may store the currently running configuration as factory defaults.
This configuration will be activated whenever a factory reset has been triggered.
Store

7.7.5. Troubleshooting

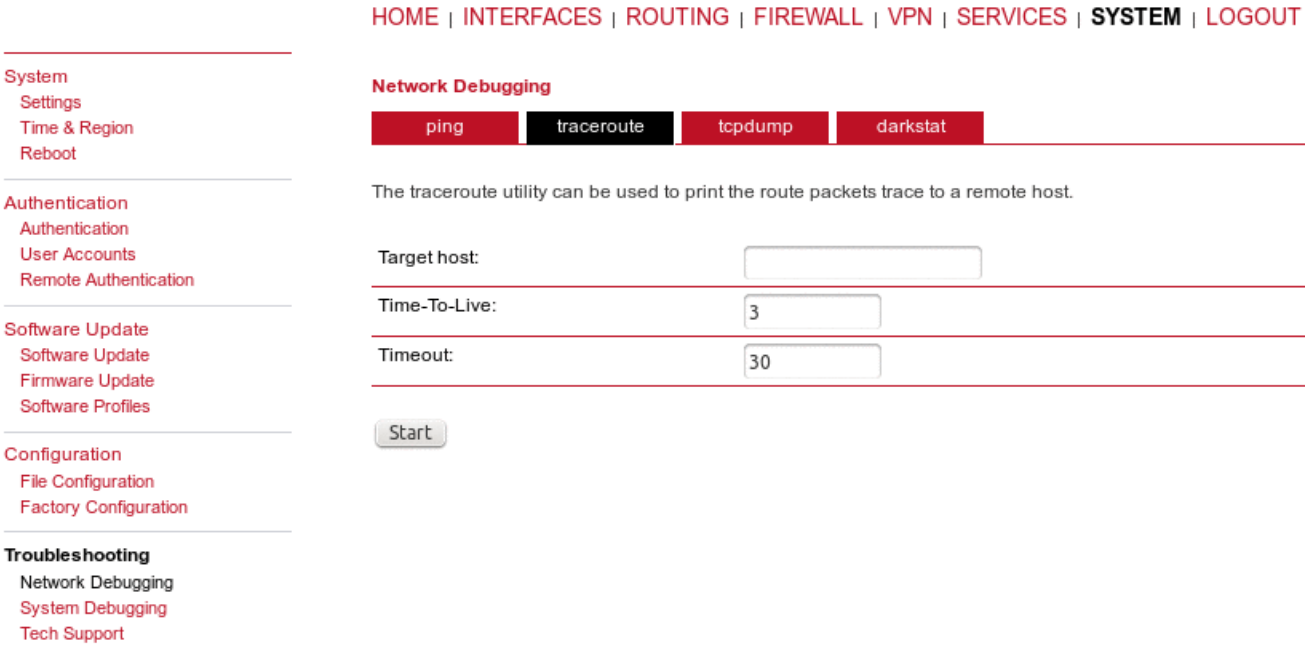
Network Debugging

Various tools reside on this page for further analysis of potential configuration issues. The **ping** utility can be used to verify the remote host reachability.



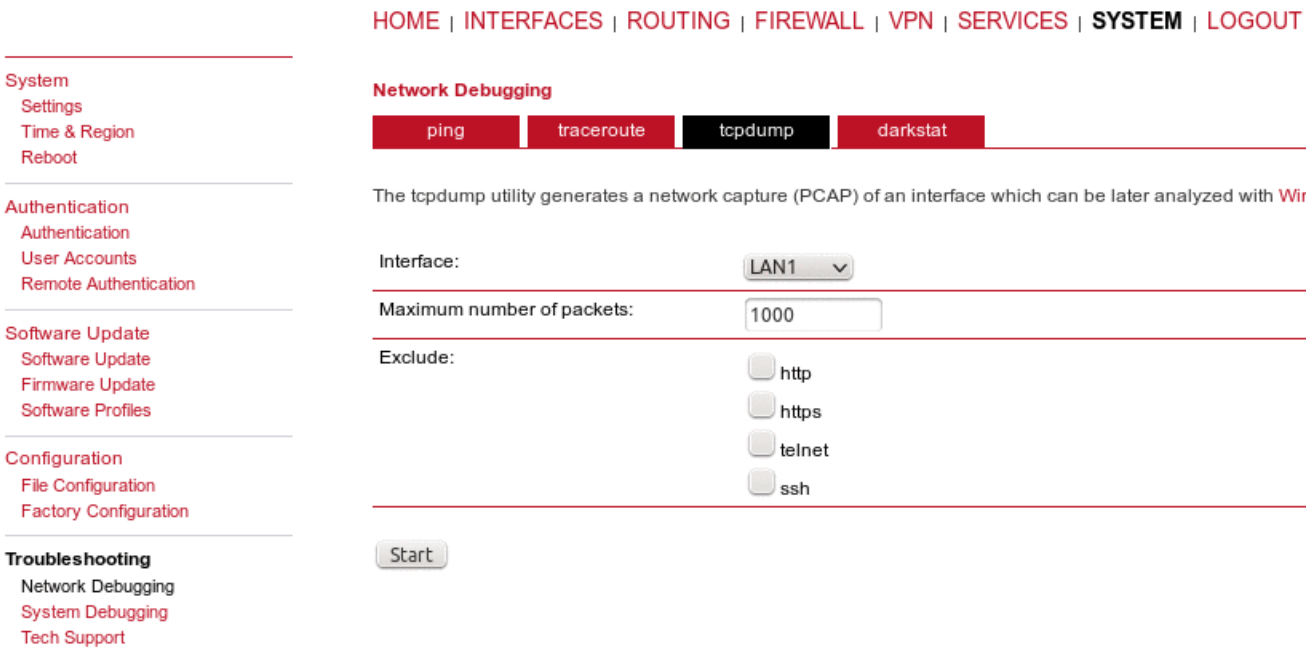
Define the remote host (IP address or hostname), number of packets and the packet size.

The **traceroute** utility can be used to print the route to a remote host.



Define the target host (IP or hostname), Time-To-Live (TTL - number of hops on the resulting route) and the timeout in seconds (max. time to wait for the final respond).

The **tcpdump** utility generates a network capture (PCAP) of an interface which can be later analyzed with Wireshark.

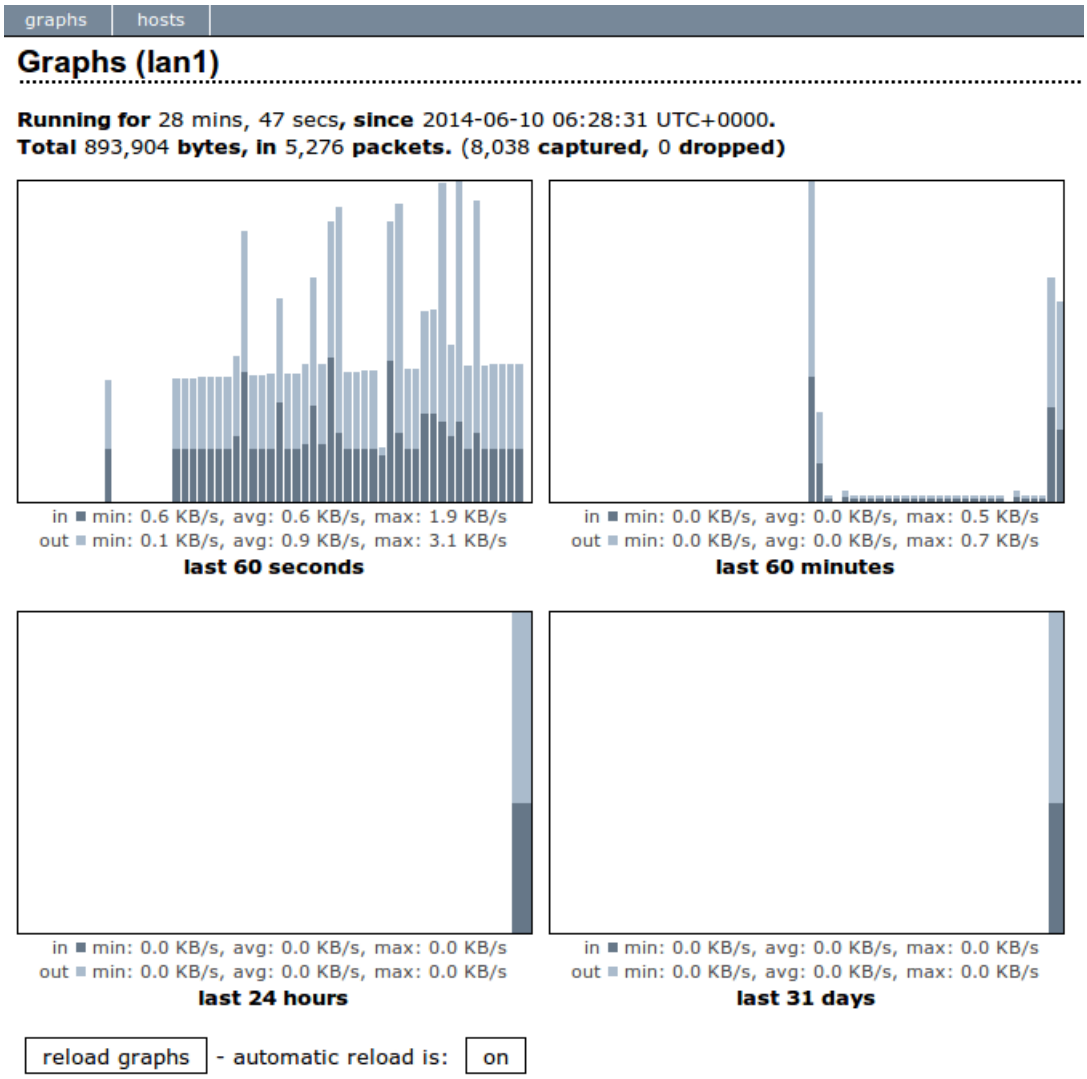


Several basic protocols can be excluded from the resulting PCAP file (HTTP, HTTPS, Telnet and SSH).

Note

The default number of received packets is set to 1000. For downloading the file, just click on the Download button. The captured file can be also downloaded from the /tmp/ directory via the appropriate file manager.

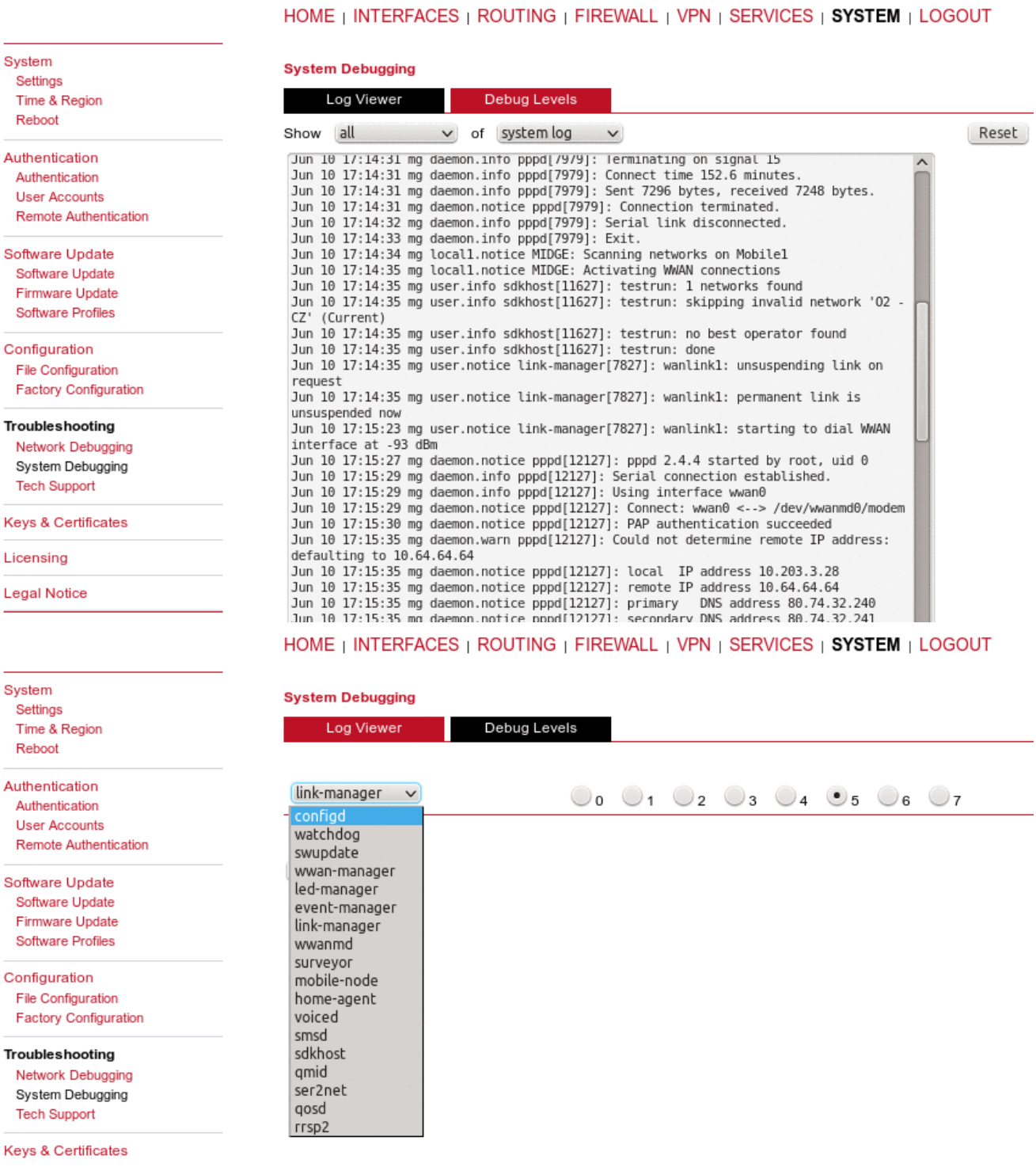
The **darkstat** utility can be used to visualize your current network connections and traffic on a particular interface.


graphs
hosts
Graphs (lan1)
Running for 28 mins, 47 secs, since 2014-06-10 06:28:31 UTC+0000.
Total 893,904 bytes, in 5,276 packets. (8,038 captured, 0 dropped)
in min: 0.6 KB/s, avg: 0.6 KB/s, max: 1.9 KB/s
out min: 0.1 KB/s, avg: 0.9 KB/s, max: 3.1 KB/s
last 60 seconds
in min: 0.0 KB/s, avg: 0.0 KB/s, max: 0.5 KB/s
out min: 0.0 KB/s, avg: 0.0 KB/s, max: 0.7 KB/s
last 60 minutes
in min: 0.0 KB/s, avg: 0.0 KB/s, max: 0.0 KB/s
out min: 0.0 KB/s, avg: 0.0 KB/s, max: 0.0 KB/s
last 24 hours
in min: 0.0 KB/s, avg: 0.0 KB/s, max: 0.0 KB/s
out min: 0.0 KB/s, avg: 0.0 KB/s, max: 0.0 KB/s
last 31 days
reload graphs
- automatic reload is:
on

After the utility initialization, it can be viewed in a separate window. Displaying graphs and individual host statistics are supported.

System Debugging

Log files can be viewed, downloaded and reset here. Please study them carefully in case of any issues.


HOME | INTERFACES | ROUTING | FIREWALL | VPN | SERVICES | SYSTEM | LOGOUT
System
Settings
Time & Region
Reboot
Authentication
Authentication
User Accounts
Remote Authentication
Software Update
Software Update
Firmware Update
Software Profiles
Configuration
File Configuration
Factory Configuration
Troubleshooting
Network Debugging
System Debugging
Tech Support
Keys & Certificates
Licensing
Legal Notice
System Debugging
Log Viewer
Debug Levels
Show all of system log
Reset
Jun 10 17:14:31 mg daemon.info pppd[7979]: Terminating on signal 15
Jun 10 17:14:31 mg daemon.info pppd[7979]: Connect time 152.6 minutes.
Jun 10 17:14:31 mg daemon.info pppd[7979]: Sent 7296 bytes, received 7248 bytes.
Jun 10 17:14:31 mg daemon.notice pppd[7979]: Connection terminated.
Jun 10 17:14:32 mg daemon.info pppd[7979]: Serial link disconnected.
Jun 10 17:14:33 mg daemon.info pppd[7979]: Exit.
Jun 10 17:14:34 mg local1.notice MIDGE: Scanning networks on Mobile1
Jun 10 17:14:35 mg local1.notice MIDGE: Activating WWAN connections
Jun 10 17:14:35 mg user.info sdkhost[11627]: testrun: 1 networks found
Jun 10 17:14:35 mg user.info sdkhost[11627]: testrun: skipping invalid network '02 - CZ' (Current)
Jun 10 17:14:35 mg user.info sdkhost[11627]: testrun: no best operator found
Jun 10 17:14:35 mg user.info sdkhost[11627]: testrun: done
Jun 10 17:14:35 mg user.notice link-manager[7827]: wanlink1: unsuspending link on request
Jun 10 17:14:35 mg user.notice link-manager[7827]: wanlink1: permanent link is unsuspended now
Jun 10 17:15:23 mg user.notice link-manager[7827]: wanlink1: starting to dial WWAN interface at -93 dBm
Jun 10 17:15:27 mg daemon.notice pppd[12127]: pppd 2.4.4 started by root, uid 0
Jun 10 17:15:29 mg daemon.info pppd[12127]: Serial connection established.
Jun 10 17:15:29 mg daemon.info pppd[12127]: Using interface wwan0
Jun 10 17:15:29 mg daemon.notice pppd[12127]: Connect: wwan0 <--> /dev/wwanmd0/modem
Jun 10 17:15:30 mg daemon.notice pppd[12127]: PAP authentication succeeded
Jun 10 17:15:35 mg daemon.warn pppd[12127]: Could not determine remote IP address: defaulting to 10.64.64.64
Jun 10 17:15:35 mg daemon.notice pppd[12127]: local IP address 10.203.3.28
Jun 10 17:15:35 mg daemon.notice pppd[12127]: remote IP address 10.64.64.64
Jun 10 17:15:35 mg daemon.notice pppd[12127]: primary DNS address 80.74.32.240
Jun 10 17:15:35 mg daemon.notice pppd[12127]: secondary DNS address 80.74.32.241
HOME | INTERFACES | ROUTING | FIREWALL | VPN | SERVICES | SYSTEM | LOGOUT
System Debugging
Log Viewer
Debug Levels
link-manager
0 1 2 3 4 5 6 7
configd
watchdog
swupdate
wwan-manager
led-manager
event-manager
link-manager
wwanmd
surveyor
mobile-node
home-agent
voiced
smsd
sdkhost
qmid
ser2net
qosd
rrsp2

Default debugging levels for individual daemons are as follows:

- configd – 4
- watchdog – 4
- swupdate – 5
- wwan-managerc – 5
- led-manager – 5

- event-manager – 5
- link-manager – 5
- wwanmd – 5
- surveyor – 5
- mobile-node – 4
- home-agent – 4
- voiced – 4
- smsd – 5
- sdkhost – 6
- qmid – 4
- ser2net – 4
- rrsp2 – 1
- qosd – 0

You can change the values to suit your needs and you can reset the values into their defaults by pressing the "**Reset**" button afterwards.

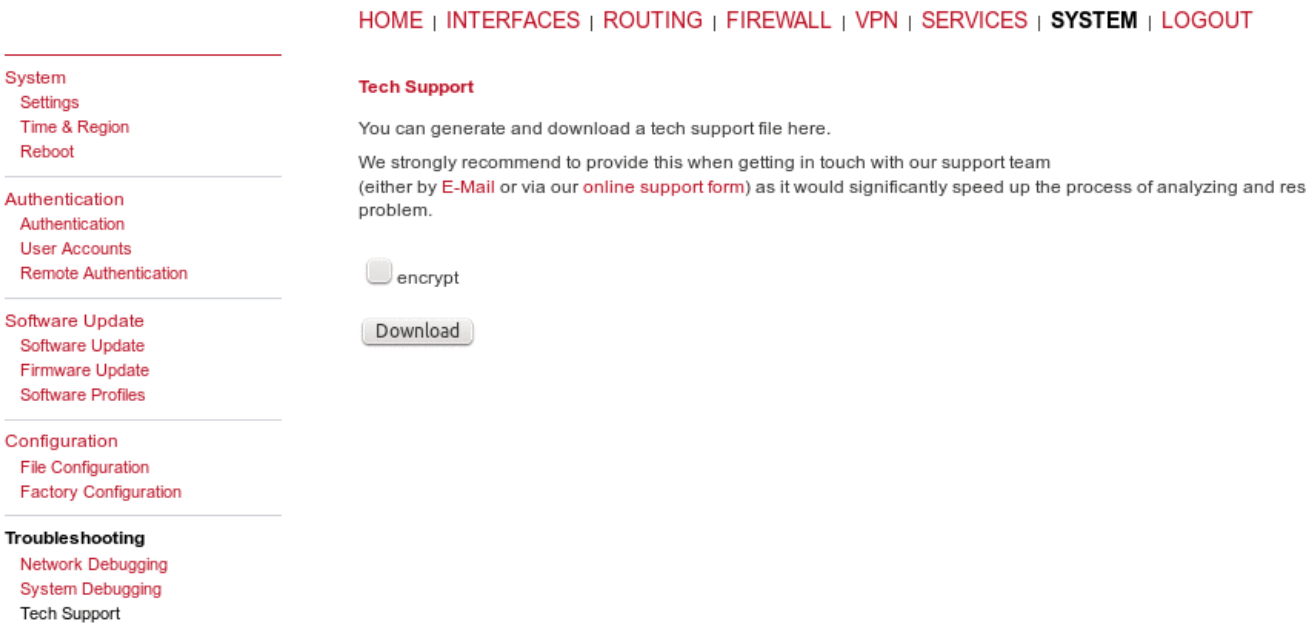
Tech Support

You can generate and download a tech support file here.

We strongly recommend providing this file when getting in touch with our support team, either by e-mail or via our online support form, as it would significantly speed up the process of analyzing and resolving your problem.

Note

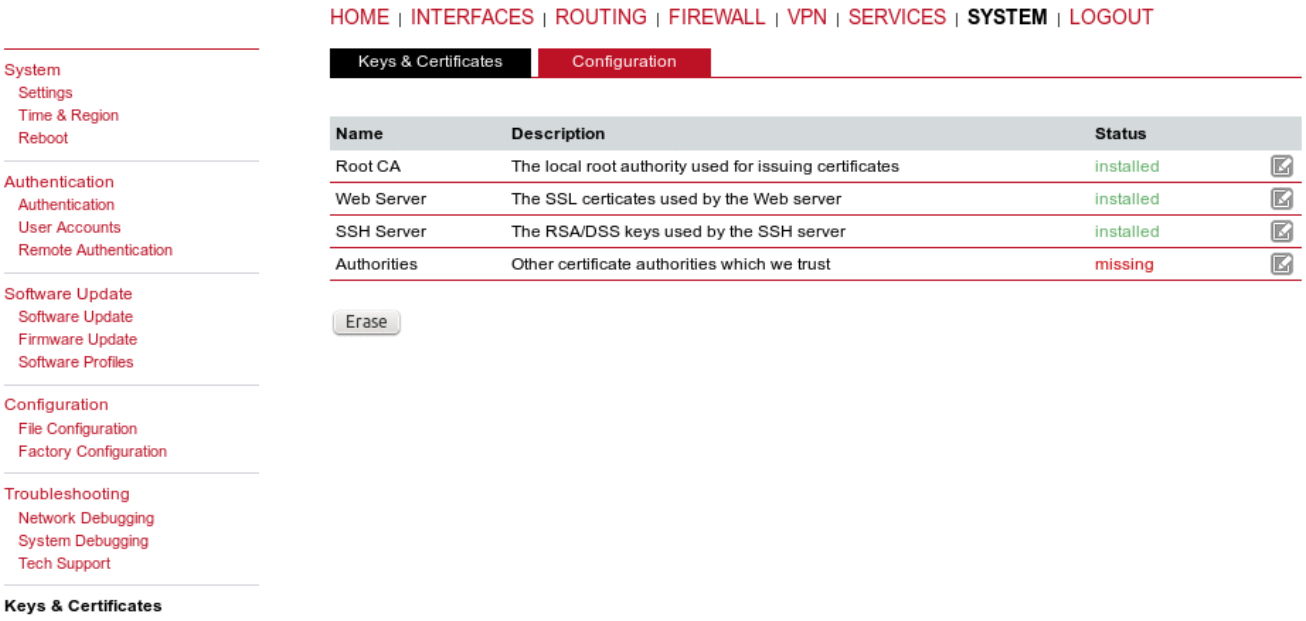
For both direct E-mail and Online support form a connection to the Internet has to be available.



You can encrypt the Techsupport file in order to secure the file against reading it without knowing the security key for decrypting the file. It is more secure way to send the techsupport file via nonsecure e-mail. The decrypting key is known by our support team only and cannot be provided to anybody.

7.7.6. Keys & Certificates

The key and certificate page lets you generate required files for securing your services (such as the HTTPS/WebServer and SSH server). Keep in mind that you will need to create keys and certificates for VPN or WLAN in case of certificate based authentication. You can also revoke and invalidate certificates again (for instance if they have been compromised or lost).



The entry pages shows an overview about installed keys and certificates. The following sections may appear:

Root CA: The root Certificate Authority (CA) which issues certificates, its key can be used to certify it at trusted third party on other systems.

Web Server: The certificates for the Web server required for running HTTP over SSL (HTTPS).

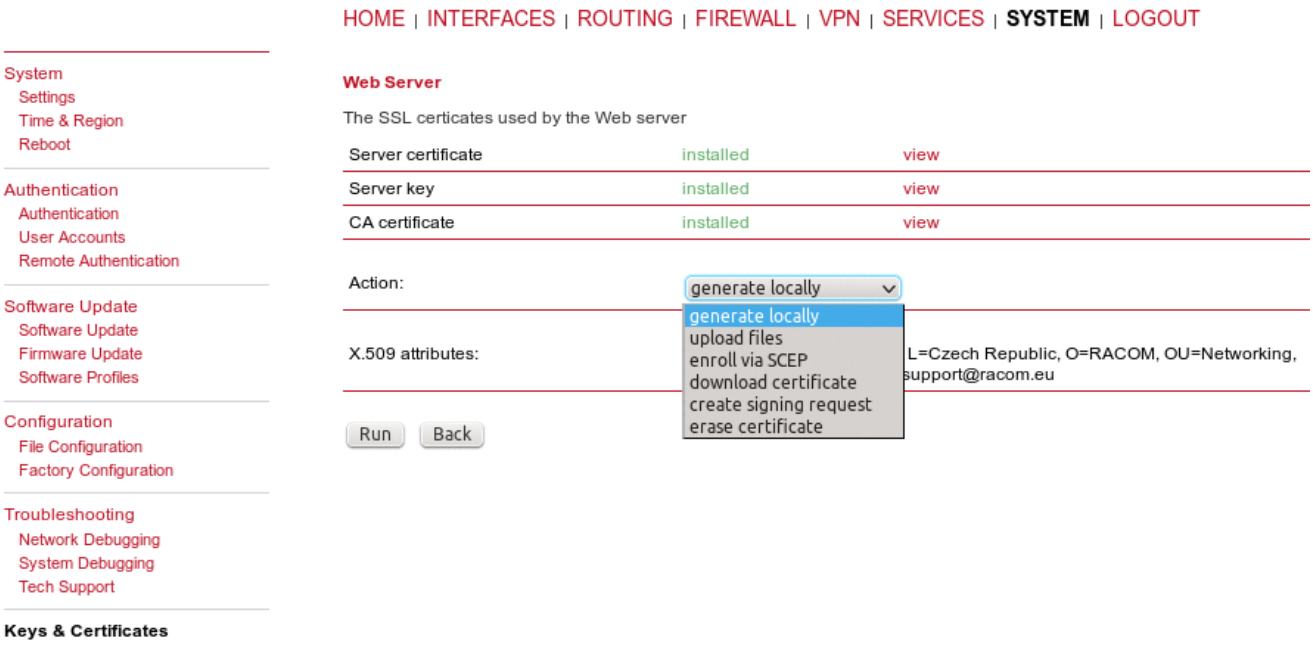
SSH Server: The DSS/DSA keys for the SSH server.

OpenVPN: Server or client keys and certificates for running OpenVPN tunnels.

IPsec: Server or client keys and certificates for running IPsec tunnels.

WLAN: Keys and certificates for implementing certificate-based WLAN authentication (e.g. WPA-EAP-TLS).

Authorities: Other certificate authorities which we trust when establishing SSL client connections.



For each certificate section it is possible to perform the following operations:

generate locally: Generate key and certificate locally on M!DGE/MG102i

upload files: Key and certificate will be uploaded. We support files in PKCS12, PKCS7, PEM/DER format as well as RSA/DSS keys in OpenSSH or Dropbear format.

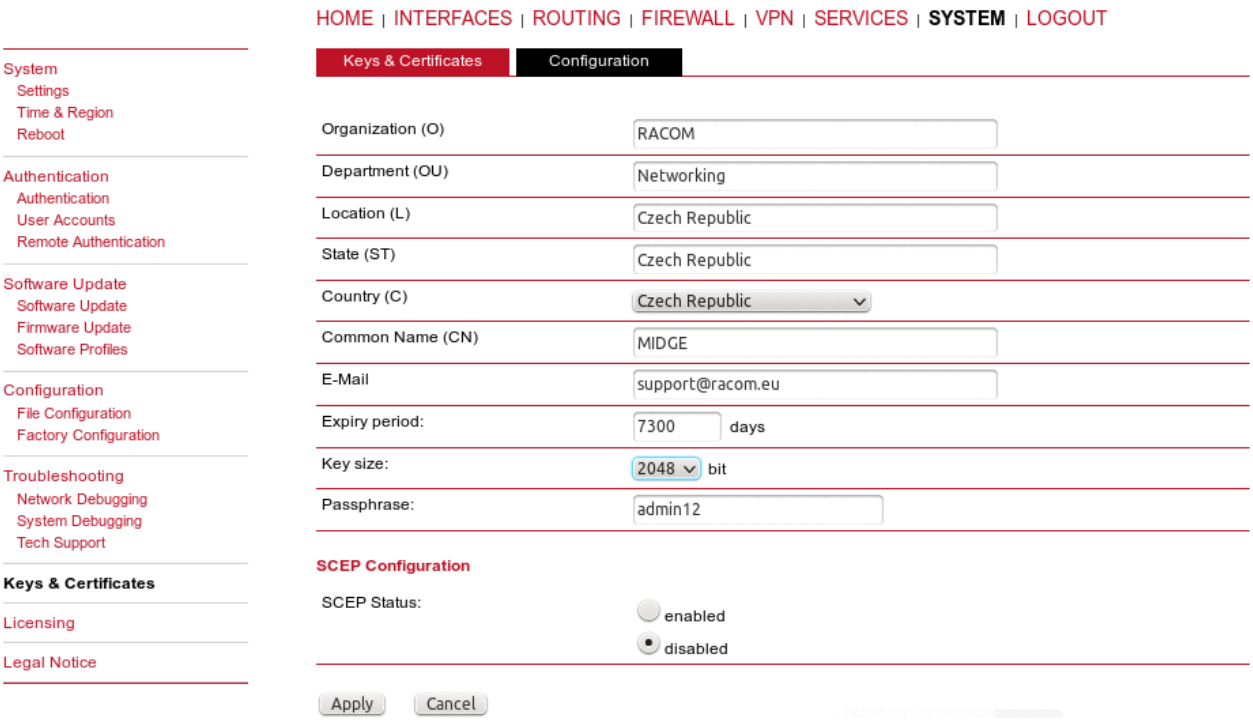
enroll via SCEP: Enroll key and certificate via SCEP

download certificate: Download key and certificate in ZIP format (files will be encoded in PEM format)

create signing request: Generate key locally and create a signing request to retrieve a certificate signed by another authority

erase certificate: Erase all keys and certificates associated with this section

Configuration



This page provides some general configuration options which will be applied when operating with keys and certificates. If keys, certificates and signing requests are generated locally, the following settings will be taken into account:

Organization (O): The certificate owner's organization

Department (OU): The name of the organizational unit to which the certificate issuer belongs

Location (L): The certificate owner's location

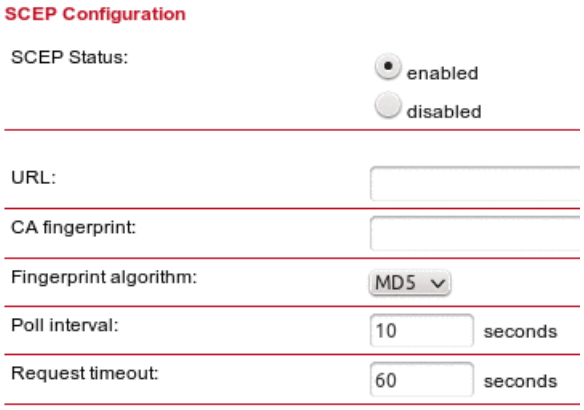
State (ST): The certificate owner's state

Country (C): The certificate owner's country (usually a TLD abbreviation)

Please be aware of the fact, that the local random number generator (RNG) provides pretty good randomness for most applications. If stronger cryptography is mandatory, we suggest to create the keys at an external RNG device or manage all certificates completely on a remote certification server. Nevertheless, using a local certificate authority can issue and manage all required certificates and also run a certificate revokation list (CRL).

When importing keys, the certificate and key file can be uploaded individually encoded in PEM/DER or PKCS7 format. All files (CA certificate, certificate and private key) can also be uploaded in one stroke by using the container format PKCS12. RSA/DSS keys can be converted from OpenSSH or Dropbear formats. It is possible to specify the passphrase for opening the private key. Please note that the system will generally apply the system-wide certificate passphrase on a key when installing the certificate. Thus, changing the general passphrase will result in all local keys getting equipped with the new one.

SCEP Configuration



If certificates are getting enrolled by using the Simple Certificate Enrollment Protocol (SCEP) the following settings can be configured:

SCEP status:	Specifies whether SCEP is enabled or not.
URL:	The SCEP URL, usually in the form http://<host>/<path>/pkiclient.exe.
CA fingerprint:	The fingerprint of the certificate used to identify the remote authority. If left empty, any CA will be trusted.
Fingerprint algorithm:	The fingerprint algorithm for identifying the CA (MD5 or SHA1).
Poll interval:	The polling interval in seconds for a certificate request.
Request timeout:	The max. polling time in seconds for a certificate request.

When enrolling certificates, the CA certificate will be initially fetched from the specified SCEP URL using the getca operation. It will be shown on the configuration page and it has to be verified that it belongs to the correct authority. Otherwise, the CA must be rejected. This part is essential when using SCEP as it builds up the chain of trust. If a certificate enrollment request times out, it is possible to re-trigger the interrupted enrollment request and it will be resumed using the previously generated key. In case a request has been rejected, you are required to erase the certificate first and then start the enrollment process all over again.

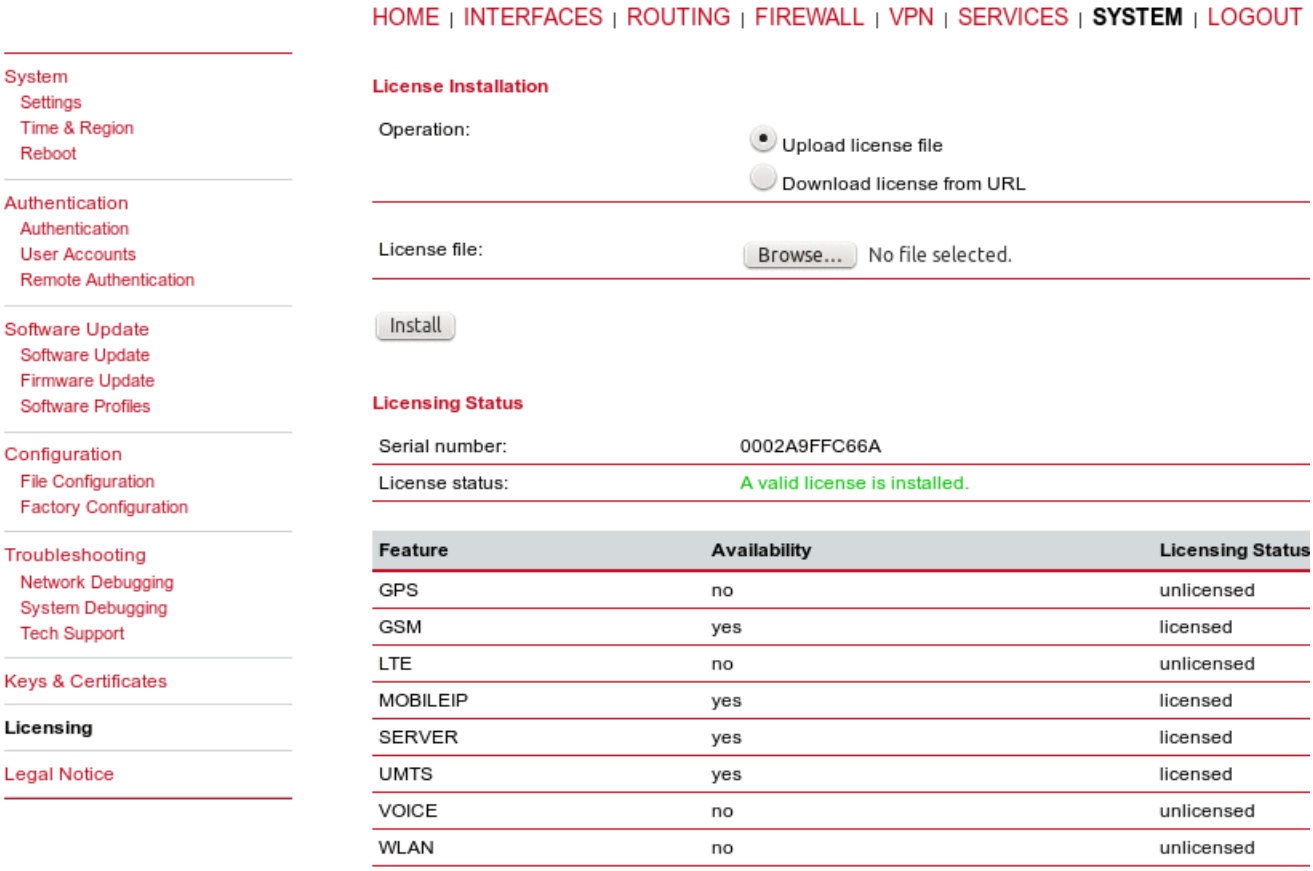
Authorities

For SSL client connections (as used by SDK functions or when downloading configuration/software images) you might upload a list of CA certificates which are considered trusted. To obtain the CA certificate from a particular site with Mozilla Firefox, the following steps will be required:

- Point the browser to the relevant HTTPS website
- Click the padlock in the address bar
- Click the More Information and the View Certificate button
- Select the Details tab and press the Export button
- Choose a path for the file (e.g. website.pem)

7.7.7. Licensing

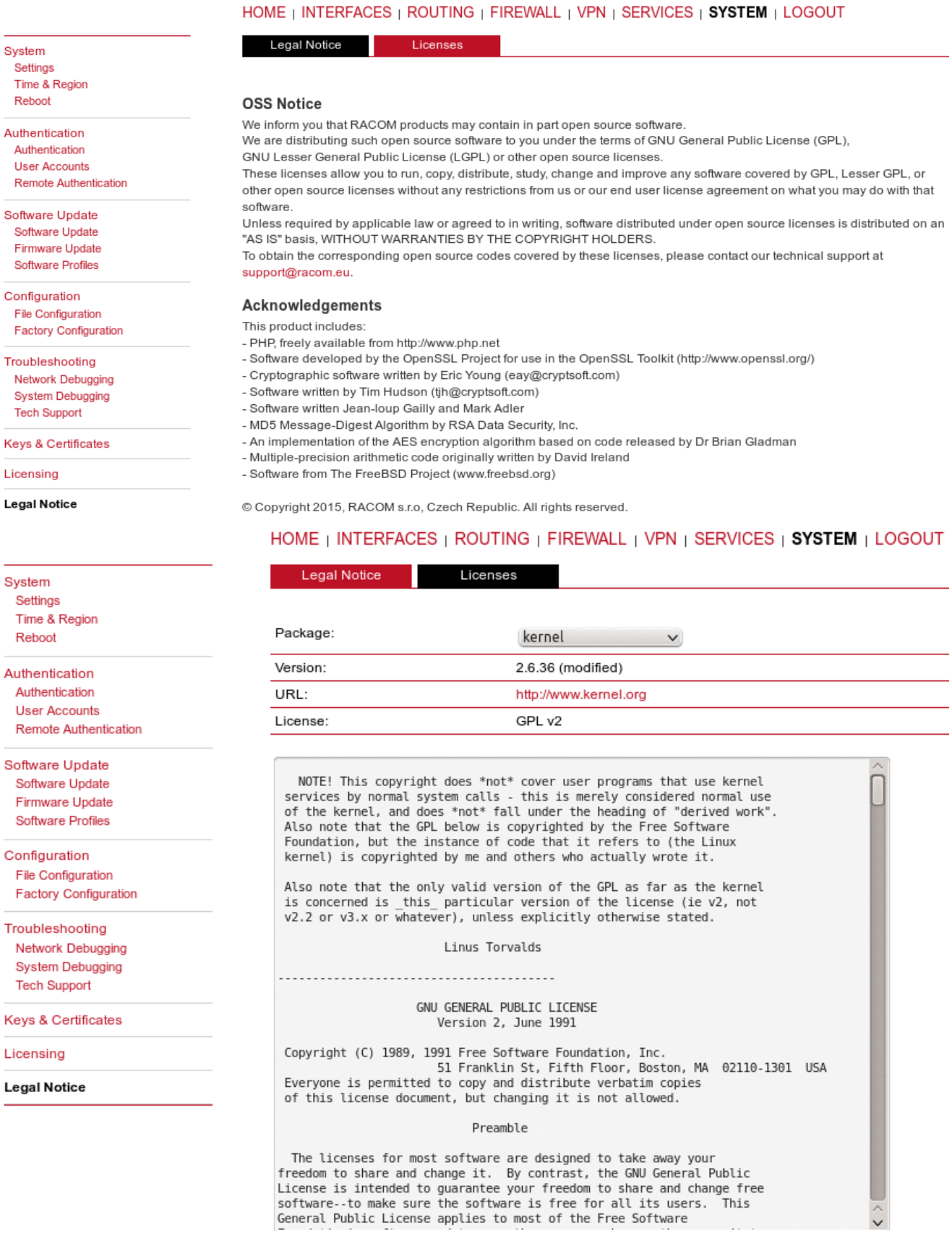
This menu allows you to view and update the license status of your system. Note that some features are disabled if no valid license is provided.



Availability means that the licence can be applied to the current hardware. The valid license is active if the status "licensed" is displayed in the respective line.

7.7.8. Legal Notice

A dedicated GUI page under SYSTEM is pointing out that M!DGE/MG102i contains in part open source software that may be licensed under GPL, LGPL or other open source licenses. It further provides detailed information for each package, including the relevant license text and the corresponding source URL. The user is now obliged to accept our end user license agreement during the initial setup of the router. We remind you that the source code of any package can be obtained by contacting our technical support at support@racom.eu.



HOME | INTERFACES | ROUTING | FIREWALL | VPN | SERVICES | **SYSTEM** | LOGOUT

Legal Notice | Licenses

System
- Settings
- Time & Region
- Reboot

Authentication
- Authentication
- User Accounts
- Remote Authentication

Software Update
- Software Update
- Firmware Update
- Software Profiles

Configuration
- File Configuration
- Factory Configuration

Troubleshooting
- Network Debugging
- System Debugging
- Tech Support

Keys & Certificates

Licensing

Legal Notice

OSS Notice

We inform you that RACOM products may contain in part open source software.
We are distributing such open source software to you under the terms of GNU General Public License (GPL), GNU Lesser General Public License (LGPL) or other open source licenses.
These licenses allow you to run, copy, distribute, study, change and improve any software covered by GPL, Lesser GPL, or other open source licenses without any restrictions from us or our end user license agreement on what you may do with that software.
Unless required by applicable law or agreed to in writing, software distributed under open source licenses is distributed on an "AS IS" basis, WITHOUT WARRANTIES BY THE COPYRIGHT HOLDERS.
To obtain the corresponding open source codes covered by these licenses, please contact our technical support at support@racom.eu.

Acknowledgements

This product includes:
- PHP, freely available from http://www.php.net
- Software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)
- Cryptographic software written by Eric Young (eay@cryptsoft.com)
- Software written by Tim Hudson (tjh@cryptsoft.com)
- Software written Jean-loup Gailly and Mark Adler
- MD5 Message-Digest Algorithm by RSA Data Security, Inc.
- An implementation of the AES encryption algorithm based on code released by Dr Brian Gladman
- Multiple-precision arithmetic code originally written by David Ireland
- Software from The FreeBSD Project (www.freebsd.org)

© Copyright 2015, RACOM s.r.o, Czech Republic. All rights reserved.

HOME | INTERFACES | ROUTING | FIREWALL | VPN | SERVICES | **SYSTEM** | LOGOUT

Legal Notice | Licenses

System
- Settings
- Time & Region
- Reboot

Authentication
- Authentication
- User Accounts
- Remote Authentication

Software Update
- Software Update
- Firmware Update
- Software Profiles

Configuration
- File Configuration
- Factory Configuration

Troubleshooting
- Network Debugging
- System Debugging
- Tech Support

Keys & Certificates

Licensing

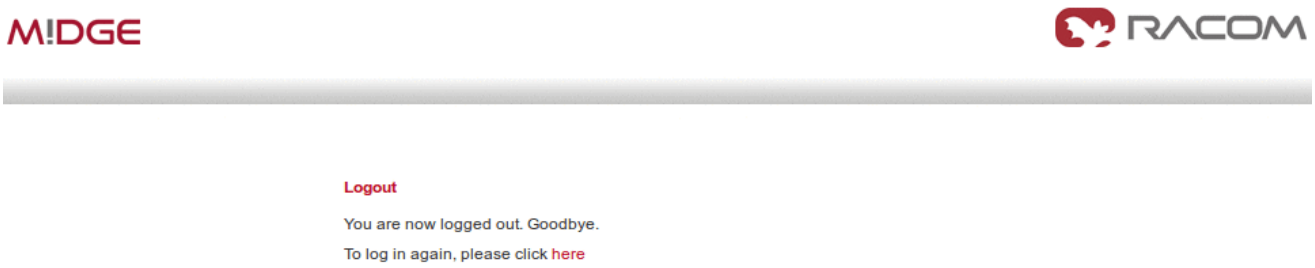
Legal Notice

Package:	kernel
Version:	2.6.36 (modified)
URL:	http://www.kernel.org
License:	GPL v2

```
  NOTE! This copyright does *not* cover user programs that use kernel
services by normal system calls - this is merely considered normal use
of the kernel, and does *not* fall under the heading of "derived work".
Also note that the GPL below is copyrighted by the Free Software
Foundation, but the instance of code that it refers to (the Linux
kernel) is copyrighted by me and others who actually wrote it.

Also note that the only valid version of the GPL as far as the kernel
is concerned is _this_ particular version of the license (ie v2, not
v2.2 or v3.x or whatever), unless explicitly otherwise stated.

                        Linus Torvalds

----------------------------------------

                    GNU GENERAL PUBLIC LICENSE
                       Version 2, June 1991

 Copyright (C) 1989, 1991 Free Software Foundation, Inc.
                       51 Franklin St, Fifth Floor, Boston, MA  02110-1301  USA
 Everyone is permitted to copy and distribute verbatim copies
 of this license document, but changing it is not allowed.

                            Preamble

  The licenses for most software are designed to take away your
freedom to share and change it.  By contrast, the GNU General Public
License is intended to guarantee your freedom to share and change free
software--to make sure the software is free for all its users.  This
General Public License applies to most of the Free Software
```

7.8. LOGOUT

Log out from Web Manager.



8. Command Line Interface

The Command Line Interface (CLI) offers a unified control interface to the router and can be used to get/set configuration parameters, apply updates, restart services or perform other system tasks.

The CLI should be started using **cli -i** command from system shell or when logging as root user. A list of available commands can be displayed by running **cli -l**. It will be started automatically in interactive mode when logging in as *admin* user.

```
$ cli
Name:
        cli (Command Line Utility)

Usage:
         [-ilvh] <command>
```

```
~ $ cli -i
MIDGE Command Line Interface (version 0.2)
(C) Copyright RACOM s.r.o, Czech Republic

Enter 'help' for a list of available commands
or hit the TAB key for auto-completion.

Ready to serve.

>
```

The CLI supports the TAB completion, that is expanding entered words or fragments by hitting the TAB key at any time. This applies to commands but also to arguments and generally offers a convenient way for working on the shell.

Please note that each CLI session will perform an automatic logout as soon as a certain time of inactivity (10 minutes by default) have been reached. It can be turned off by the command `no-autologout`.

The CLI can be exited by running `exit`.

8.1. General usage

When operating the `CLI` in interactive mode, each entered command will be executed by the `RETURN` key. You can use the `Left` and `Right` keys to move the current point between entered characters or use the `Up` and `Down` keys to search the history of entered commands. Pressing `CTRL-c` twice or `CTRL-d` on an empty command line will exit the `CLI`.

List of supported key sequences:

Key Sequence	Action
CTRL-a	Move to the start of the current line.
CTRL-e	Move to the end of the line.
CTRL-f	Move forward a character.

Key Sequence	Action
CTRL-b	Move back a character.
ALT-f	Move forward to the end of the next word.
ALT-b	Move back to the start of the current or previous word.
CTRL-l	Clear the screen leaving the current line at the top of the screen, with an argument given refresh the current line without clearing the screen.
CTRL-p	Fetch the previous command from the history list, moving back in the list.
CTRL-n	Fetch the next command from the history list, moving forward in the list.
ALT-<	Move to the first line in the history.
ALT->	Move to the end of the input history.
CTRL-r	Search backward starting at the current line and moving up through the history.
CTRL-s	Session will be frozen.
CTRL-q	Reactivate frozen session.
CTRL-d	Delete character at point or exit CLI if at the beginning of the line.
CTRL-t	Drag the character before point forward moving point forward as well. If point is at the end of the line, then this transposes the two characters before point.
ALT-t	Drag the word before point past the word after point, moving point over that word as well. If point is at the end of the line, this transposes the last two words on the line.
CTRL-k	Delete the text from point to the end of the line.
CTRL-y	Yank the top of the deleted text into the buffer at point.

Please note, that it can be required to apply quotes (") when entering commands with arguments containing whitespaces.

The following sections are trying to explain the available commands.

8.2. Print help

The `help` command can be used to get the list of available commands when called without arguments, otherwise it will print the usage of the specified command.

```
> help
Usage:
        help [<command>]

Available commands:

        get                 Get config parameters
        set                 Set config parameters
        update              Update system facilities
        cert                Manage keys and certificates
        status              Get status information
        scan                Scan networks
        send                Send message, mail, techsupport or ussd
        restart             Restart service
        debug               Debug system
        reset               Reset system facilities
        reboot              Reboot system
        shell               Run shell command
        help                Print help for command
        no-autologout       Turn off auto-logout
        history             Show command history
        exit                Exit
```

8.3. Getting config parameters

The **get** command can be used to get configuration values (not the current values).

```
get -h
Usage:
        get [-hsvfc] <parameter> [<parameter>..]

Options:
        -s        generate sourceable output
        -v        validate config parameter
        -f        get factory default rather than current value
        -c        show configuration sections
```

See the following example for reading configuration DIO values:

```
> get dio.out1
dio.out1=on
> get dio.out2
dio.out2=on
```

8.4. Setting config parameters

The **set** command can be used to set configuration values.

```
> set -h
Usage:
```

```
        set [-hv] <parameter>=<value> [<parameter>=<value>..]

Options:
        -v     validate config parameter
```

See the following example for setting configuration digital output values. Both values will be "off" and both values will be also "off" after the next start-up procedure.

```
> set dio.out1=off
> set dio.out2=off
```

8.5. Updating system facilities

The **update** command can be used to perform various system updates.

```
> update -h
Usage:
        update [-hfrsn] <software|config|license|sshkeys> <URL>

Options:
        -r     reboot after update
        -f     force update
        -n     don't reset missing config values with factory defaults
        -s     show update status

Available update targets:

        software           Perform software update
        firmware           Perform module firmware update
        config             Update configuration
        license            Update licenses
        sshkeys            Install SSH authorized keys
```

8.6. Manage keys and certificates

The **update** command can be used to manage keys and certificates.

```
> cert -h
Usage:
        cert [-h] [-p phrase] <operation> <cert> [<url>]

Possible operations:

        install           install a certificate from specified URL
        create            create a certificate locally
        enroll            enroll a certificate via SCEP
        erase             erase an installed certificate
        view              view an installed certificate
```

8.7. Getting status information

The **status** command can be used to get various status information of the system.

```
> status -h
Usage:
        status [-hs] <section>

Options:
        -s     generate sourceable output

Available sections:

        summary              Short status summary
        info                 System and config information
        config               Current configuration
        system               System information
        configuration        Configuration information
        license              License information
        wwan                 WWAN module status
        wlan                 WLAN module status
        gnss                 GNSS (GPS) module status
        eth                  Ethernet interface status
        lan                  LAN interface status
        wan                  WAN interface status
        openvpn              OpenVPN connection status
        ipsec                IPsec connection status
        pptp                 PPTP connection status
        gre                  GRE connection status
        dialin               Dial-In connection status
        mobileip             MobileIP status
        dio                  Digital IO status
        audio                Audio module status
        can                  CAN module status
        uart                 UART module status
        redundancy           Redundancy status
        sms                  SMS status
        firewall             Firewall status
        qos                  QoS status
        neigh                Neighborhood status
        location             Current Location
```

In the following example, we read the current DIO values. Remember that the current states do not correspond to the configuration values set with "set dio.out" commands.

```
> status dio
=== DIGITAL IO INFORMATION ===
IN1:                            off
IN2:                            on
OUT1:                           on
OUT2:                           off
```

8.8. Scan

The **scan** command can be used to scan the mobile network for the possible networks. Note that the active mobile connection will be deactivated during the scan procedure.

```
> scan -h
Usage:
        scan [-hs] <interface>

Options:
        -s     generate sourceable output

Available interfaces:

        Mobile1    (wwan0)
```

See the example below:

```
> scan -s Mobile1

NETWORK1_NAME="O2 - CZ"
NETWORK1_TECH="3G"
NETWORK1_LAI="23002"
NETWORK1_RAT="UTRAN"
NETWORK1_STATUS="Current"

NETWORK_COUNT="1"
```

8.9. Sending e-mail or SMS

The **send** command can be used to send a message via E-Mail/SMS to the specified address or phone number.

```
> send -h
Usage:
        send [-h] <type> <dest> <msg>

Options:
        <type>     type of message to be sent (mail, sms, techsupport, ussd)
        <dest>     destination of message (mail-address, phone-number or argument)
        <msg>      message to be sent
```

8.10. Restarting services

The **restart** command can be used to restart system services.

```
> restart -h
Usage:
        restart [-h] <service>
```

```
Available services:

        configd             Configuration daemon
        dnsmasq             DNS/DHCP server
        dropbear            SSH server
        firewall            Firewall and NAPT
        gpsd                GPS daemon
        gre                 GRE connections
        ipsec               IPsec connections
        lighttpd            HTTP server
        link-manager        WAN links
        network             Networking
        openvpn             OpenVPN connections
        pptp                PPTP connections
        qos                 QoS daemon
        smsd                SMS daemon
        snmpd               SNMP daemon
        surveyor            Supervision daemon
        syslog              Syslog daemon
        telnet              Telnet server
        usbipd              USB/IP daemon
        voiced              Voice daemon
        vrrpd               VRRP daemon
        wlan                WLAN interfaces
        wwan-manager        WWAN manager
```

8.11. Debug

The **debug** command can be used to display individual daemons debugging output.

```
> debug -h
Usage:
        debug [-hr] [-l <level>] <target>

Options:
        -l <level>      set debug level
        -r              reset debug level

Available debug targets:

        system
        scripts
        configd
        watchdog
        swupdate
        wwan-manager
        led-manager
        event-manager
        link-manager
        wwanmd
        surveyor
```

```
        mobile-node
        home-agent
        voiced
        smsd
        sdkhost
        qmid
        ser2net
        qosd
        rrsp2
```

8.12. Resetting system

The **reset** command can be used to reset the router back to factory defaults.

```
> reset -h
Usage:
        reset [-h] [facility]

Available reset facilities:

        factory             Reset system to factory defaults
        statistics          Reset link statistics
```

8.13. Rebooting system

The **reboot** command can be used to reboot the router.

```
> reboot -h
Usage:
        reboot [-h]
```

8.14. Running shell commands

The **shell** command can be used to execute a system shell and run any arbitrary application.

```
> shell -h
Usage:
        shell [-h] [<cmd>]
```

8.15. CLI commands history

The **history** command displays the history of CLI commands entered on the unit.

```
> history
   1  help
   2  get -h
   3  get dio.out1
   4  set dio.out1=off
```

```
5  set dio.out2=off
6  set dio.out1=on
7  get dio.out1
8  get dio.out2
9  set -h
```

8.16. CLI–PHP

CLI-PHP, an HTTP front-end to the CLI application, can be used to configure and control the router remotely. It is enabled in factory configuration, thus can be used for deployment purposes, but disabled as soon as the admin account has been set up. The service can later be turned on/off by setting the cliphp.status configuration parameter:

```
> get cliphp.status
cliphp.status=0

> set cliphp.status=1
> get cliphp.status
cliphp.status=1
```

```
cliphp.status=0          Service is disabled
cliphp.status=1          Service is enabled
```

This section describes the CLI-PHP interface for Version 2, the general usage (GET requests) is defined as follows:

```
Usage:
    http (s)://cli.php?<key1>=<value1>&<key2>=<value2>..<keyN>=<
    valueN>
Available keys:
output             Output format ( html, plain )
usr                Username to be used for authentication
pwd                Password to be used for authentication
commandV           Command to be executed
arg0..arg31        Arguments passed to commands
Notes:
    The commands correspond to CLI commands as seen by 'cli -l', the arguments
   (arg0..arg31) will be directly passed to the cli application

    Thus, an URL containing the following sequence:

      command=get&arg0=admin.password&arg1=admin.debug&arg2=admin.access

   will lead to cli being called as:

    $ cli get "admin.password" "admin.debug" "admin.access"

    It supports whitespaces but please be aware that any special characters in the URL
    must be specified according to RFC1738 (which usually done by common clients such
    as wget, lynx, curl).
```

```
Response:
    The returned response will always contain a status line in the format:

    <return>: <msg>

    with return values of OK if succeeded and ERROR if failed. Any output from the
    commands will be appended

Examples:

    OK: status command successful
    ERROR: authentication failed
```

status – Display status information

```
Key usage:
        command=status[&arg0=<section>]
Notes:
        Available sections can be retrieved by running command=status&arg0=-h.
        System status can be displayed without authentication.

Examples:

http://192.168.1.1/cli.php?version=2&output=html&usr=admin&pwd=admin01&command=
status&arg0=-h
http://192.168.1.1/cli.php?version=2&output=html&usr=admin&pwd=admin01&command=
status&arg0=summary
http://192.168.1.1/cli.php?version=2&output=html&command=status
```

get – Get configuration parameter

```
Key usage:

        command=get&arg0=<config-key>[&arg1=<config-key>..]

Examples:

http://192.168.1.1/cli.php?version=2&output=html&usr=admin&pwd=
admin01&command=get&arg0=config.version

http://192.168.1.1/cli.php?version=2&output=html&usr=admin&pwd=
admin01&command=get&arg0=openvpn.status&arg1=snmp.status&arg2=ipsec.status
```

set – Set configuration parameter

```
Key usage:
     command=set&arg0=<config-key>&arg1=<config-value>[&arg2=<config
     -key>&arg3=<config-value>..]
Notes:
     In contrast to the other commands, this command requires a set
```

```
     of tuples because of the reserved '=' char, i.e.
     [arg0=key0, arg1=val0], [arg2=key1, arg3=val1], [arg4=key2, arg5=val2], etc

Examples:


http://192.168.1.1/cli.php?version=2&output=html&usr=admin&pwd=
admin01&command=set&arg0=snmp.status&arg1=1

http://192.168.1.1/cli.php?version=2&output=html&usr=admin&pwd=
admin01&command=set&arg0=snmp.status&arg1=0&arg2=openvpn.status&arg3=1
```

restart – Restart a system service

```
Key usage:
     command=restart&arg0=<service>
Notes:
     Available services can be retrieved by running 'command=restart&arg0=-h'

Examples:


http://192.168.1.1/cli.php?version=2&output=html&usr=admin&pwd=
admin01&command=restart&arg0=-h

http://192.168.1.1/cli.php?version=2&output=html&usr=admin&pwd=
admin01&command=restart&arg0=link-manager
```

reboot - Trigger system reboot

```
Key usage:
     command=reboot

Examples:


http://192.168.1.1/cli.php?version=2&output=html&usr=admin&pwd=admin01&command=reboot
```

reset - Run factory reset

```
Key usage:
     command=reset

Examples:


http://192.168.1.1/cli.php?version=2&output=html&usr=admin&pwd=admin01&command=reset
```

update - Update system facilities

```
Key usage:
     command=update&arg0=<facility>&arg1=<URL>
Notes:
     Available facilities can be retrieved by running 'command=update
&arg0=-h'

Examples:

http://192.168.1.1/cli.php?version=2&output=html&usr=admin&pwd=127
admin01&command=update&arg0=software&arg1=tftp://192.168.1.254/latest

http://192.168.1.1/cli.php?version=2&output=html&usr=admin&pwd=
admin01&command=update&arg0=config&arg1=tftp://192.168.1.254/user-
config.zip

http://192.168.1.1/cli.php?version=2&output=html&usr=admin&pwd=
admin01&command=update&arg0=license&arg1=http://192.168.1.254/xxx.lic
```

send - Send SMS

```
Key usage:
     command=send&arg0=sms&arg1=<number>&arg2=<text>
Notes:
     The phone number has to be specified in international format such
as +123456789 including a leading plus sign (which can be encoded with \%2B).
The SMS daemon must be properly configured prior to using that function.

Examples:

http://192.168.1.1/cli.php?version=2&output=html&usr=admin&pwd=admin01
&command=send&arg0=sms&arg1=\%2B123456789&arg2=test
```

send - Send E-Mail

```
Key usage:
     command=send&arg0=mail&arg1=<address>&arg2=<text>
Notes:
     The address has to be a valid E-Mail address such as abc@abc.com
(the at-sign can be encoded with \%40). The E-Mail client must be properly
configured prior to using that function.

Examples:

http://192.168.1.1/cli.php?version=2&output=html&usr=admin&pwd=admin01&
command=send&arg0=mail&arg1=abc\%40abc . com&arg2=test
```

send - Send TechSupport

```
Key usage:
     command=send&arg0=techsupport&arg1=stdout
command=send&arg0=techsupport&arg1=<address>&arg2=<subject>
Notes:
     The address has to be a valid E-Mail address such as abc@abc.com
(the at-sign can be encoded with \%40) . The E-Mail client must be properly
configured prior to using that function. In case of stdout , the downloaded
techsupport file will be called 'download'.


Examples:

http://192.168.1.1/cli.php?version=2&output=mime&usr=admin&pwd=admin01&
command=send&arg0=techsupport&arg1=stdout

http://192.168.1.1/cli.php?version=2&output=html&usr=admin&pwd=admin01&
command=send&arg0=techsupport&arg1=abc\%40abc.com&arg2=subject
```

send - Send USSD code

```
Key usage:
     command=send&arg0=ussd&arg1=<card>&arg2=<code>
Notes:
     The argument card specifies the card module index (e.g. 0 for wwan0 ).
The USSD code can consist of digits , plus signs , asterisks
(can be encoded with \%2A) and dashes (can be encoded with \%23) .


Examples:

http://192.168.1.1/cli.php?version=2&output=html&usr=admin&pwd=admin01&
command=send&arg0=ussd&arg1=0&arg2=\%2A100\%23
```

9. Troubleshooting

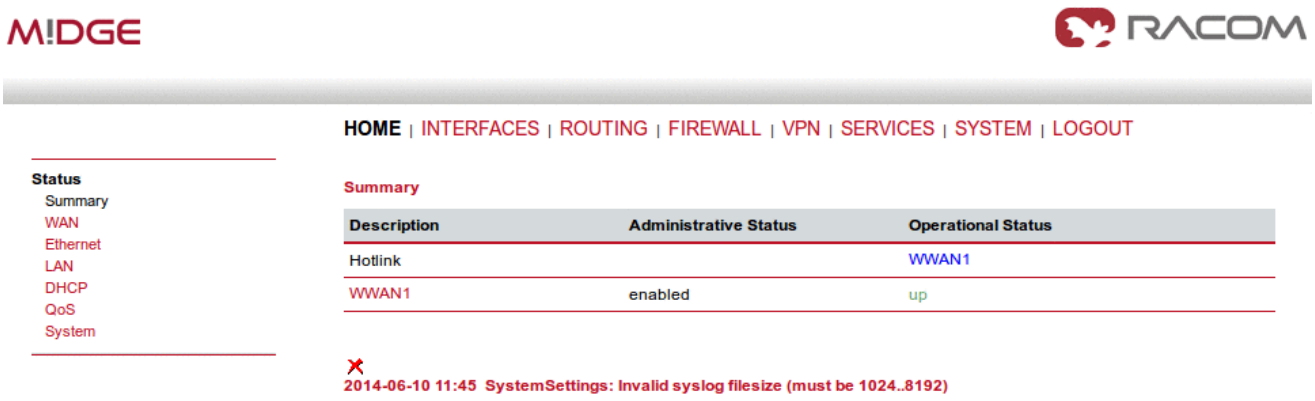
9.1. Common errors

With GPRS/UMTS connection (even if GSM signal is good enough) following Errors are common:

SIM missing	Check the SIM card status in the INTERFACES → SIMs menu, turn off the unit, insert/re-insert the SIM card and power up the unit again
PIN code required	Insert the correct PIN code in the INTERFACES → SIMs → Configuration menu
Connection not established or failed	See the SYSTEM → Troubleshooting → System Debugging output for any errors/warnings

9.2. Messages

The Web Manager displays messages in the status bar in the footer of a web page.



There are three levels:

Green	The action was performed successfully.
Yellow	Warning – please consider the information.
Red	Error – command was not performed, typically with recommended action which is required before the possible successful action.

9.3. Troubleshooting tools

9.3.1. Pinger

Connection from the M!DGE/MG102i router can be checked using the built-in pinger available in the **SYSTEM → Troubleshooting → Network Debugging menu**.

The traceroute command is available in the same menu for tracing the packets from the M!DGE/MG102i router to the Host.

9.3.2. Log Files

Information about boot-up process and about running processes can be found in the Linux-like Log files, see the **SYSTEM→ Troubleshooting → System Debugging menu**.

10. Safety, environment, licensing

10.1. Safety instructions

The M!DGE/MG102i Wireless Router must be used in compliance with any and all applicable international and national laws and in compliance with any special restrictions regulating the utilization of the communication module in prescribed applications and environments.

To prevent possible injury to health and damage to appliances and to ensure that all the relevant provisions have been complied with, use only the original accessories. Unauthorized modifications or utilization of accessories that have not been approved may result in the termination of the validity of the guarantee.

The M!DGE/MG102i Wireless Routers must not be opened. Only the replacement of the SIM card is permitted.

Voltage at all connectors of the communication module is limited to SELV (Safety Extra Low Voltage) and must not be exceeded.

For use with certified (CSA or equivalent) power supply, which must have a limited and SELV circuit output. The M!DGE/MG102i is designed for indoor use only. Do not expose the communication module to extreme ambient conditions. Protect the communication module against dust, moisture and high temperature.

We remind the users of the duty to observe the restrictions concerning the utilization of radio devices at petrol stations, in chemical plants or in the course of blasting works in which explosives are used. Switch off the communication module when traveling by plane.

When using the communication module in close proximity of personal medical devices, such as cardiac pacemakers or hearing aids, you must proceed with heightened caution.

If it is in the proximity of TV sets, radio receivers and personal computers, M!DGE/MG102i Wireless Router may cause interference.

It is recommended that you should create an approximate copy or backup of all the important settings that are stored in the memory of the device.

You must not work at the antenna installation during a lightning.

Always keep a distance bigger than 40cm from the antenna in order to keep your exposure to electromagnetic fields below the legal limits. This distance applies to Lambda/4 and Lambda/2 antennas. Larger distances apply for antennas with higher gain.

Adhere to the instructions documented in this user's manual.

10.1.1. Declaration of Conformity

CE

RACOM declares that under our own responsibility the products M!DGE/MG102i Wireless Routers comply with the relevant standards following the provisions of the Council Directive 1999/5/EC.

10.1.2. RoHS and WEEE compliance

RoHS compliant

The M!DGE/MG102i is fully compliant with the European Commission‟s RoHS (Restriction of Certain Hazardous Substances in Electrical and Electronic Equipment) and WEEE (Waste Electrical and Electronic Equipment) environmental directives).

Restriction of hazardous substances (RoHS)

The RoHS Directive prohibits the sale in the European Union of electronic equipment containing these hazardous substances: lead, cadmium, mercury, hexavalent chromium, polybrominated biphenyls (PBBs), and polybrominated diphenyl ethers (PBDEs).

End-of-life recycling programme (WEEE)

In accordance with the requirements of the council directive 2002/96/EC on Waste Electronical and Electronic Equipment (WEEE), ensure that at end-of-life you separate this product from other waste and scrap and deliver it to the WEEE collection system in your country for recycling.

10.2. Country of Origin

RACOM
RADIO DATA NETWORKS

Country of Origin Declaration

Manufacturer:	**RACOM**
Address:	**Mirova 1283, 592 31 Nove Mesto na Morave, Czech Republic**
VAT No:	**CZ46343423**

We, the manufacturer, hereby declare that Country of Origin of all the GSM products and its accessories is the Czech Republic, EU.

Part Number	Description
MG102i-L	dual SIM GPRS/EDGE/HSPA+/LTE router - 5Eth, RS232, 2DI, 2DO
MG102i-U	dual SIM GPRS/EDGE/UMTS/HSPA router - 5Eth, RS232, 2DI, 2DO
MG102i-2UW-G	dual module GPRS/EDGE/UMTS/HSPA router + WiFi + GPS
MG102_DINSET	DIN rail mounting accessories
M!DGE-UMTS	GPRS/EDGE/UMTS/HSPA router, 2Eth, RS232, 2DI, 2DO, DIN rail
M!DGE-LTE	GPRS/EDGE/HSPA/LTE router, 2Eth, RS232, 2DI, 2DO, DIN rail

Nove Mesto na Morave, 1 of March 2014
Jiri Hruska, CEO

RACOM s.r.o. • Mirova 1283 • 592 31 Nove Mesto na Morave • Czech Republic
Tel.: +420 565 659 511 • Fax: +420 565 659 512 • E-mail: racom@racom.eu

www.racom.eu

ver. 1.0

Fig. 10.1: Country of Origin declaration

10.3. Warranty

RACOM-supplied parts or equipment ("equipment") is covered by warranty for inherently faulty parts and workmanship for a warranty period as stated in the delivery documentation from the date of dispatch to the customer. The warranty does not cover custom modifications to software. During the warranty period RACOM shall, on its option, fit, repair or replace ("service") faulty equipment, always provided that malfunction has occurred during normal use, not due to improper use, whether deliberate or accidental, such as attempted repair or modification by any unauthorised person; nor due to the action of abnormal or extreme environmental conditions such as overvoltage, liquid immersion or lightning strike.

Any equipment subject to repair under warranty must be returned by prepaid freight to RACOM direct. The serviced equipment shall be returned by RACOM to the customer by prepaid freight. If circumstances do not permit the equipment to be returned to RACOM, then the customer is liable and agrees to reimburse RACOM for expenses incurred by RACOM during servicing the equipment on site. When equipment does not qualify for servicing under warranty, RACOM shall charge the customer and be reimbursed for costs incurred for parts and labour at prevailing rates.

This warranty agreement represents the full extent of the warranty cover provided by RACOM to the customer, as an agreement freely entered into by both parties.

RACOM warrants the equipment to function as described, without guaranteeing it as befitting customer intent or purpose. Under no circumstances shall RACOM's liability extend beyond the above, nor shall RACOM, its principals, servants or agents be liable for any consequential loss or damage caused directly or indirectly through the use, misuse, function or malfunction of the equipment, always subject to such statutory protection as may explicitly and unavoidably apply hereto.

Appendix A. Glossary

APN	Access Point Name / Access Point Node
CE	Conformity of equipment according to EU rules
CS	Coding Scheme
CSD	Circuit Switched Data
DHCP	Dynamic Host Configuration Protocol
DMZ	Demilitarized Zone
DNS	Domain Name System
EDGE	Enhanced Data Service for GSM Evolution
EMC	Electromagnetic compatibility
FTP	File Transfer Protocol
GPRS	General Packet Radio Service
GSM	Global System for Mobile communications
GUI	Graphical User Interface
HSCSD	High Speed Circuit Switched Data
HSDPA	High-Speed Downlink Packet Access
HSUPA	High-Speed Uplink Packet Access
HTML	Hypertext Markup Language
HW	Hardware
IP	Internet Protocol
IPsec	Internet Protocol Security
ISDN	Integrated Services Digital Network
ISP	Internet Service Provider
LAN	Local Area Network
NAPT	Network Address Port Translation
NAT	Network Address Translation
POP	Point of Presence
POP, POP3	Post Office Protocol, Version 3
PPP	Point to Point Protocol

RAS	Remote Access Service (Dial-in Networking PPP)
RoHS	Restriction of hazardous substances
SIM	Subscriber Identity Module
SW	Software
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
UDP	User Datagram Protocol
UMTS	Universal Mobile Telecommunications System
URL	Universal Resource Locator
VPN	Virtual Private Network
WEEE	Waste Electrical and Electronic Equipment environmental directives

Index

A
accessories, 18
antenna
  GSM/UMTS, 20
  mounting, 22
authentication, 103

B
basic setup, 21
brc
  COM, 41

C
certificates, 115
CLI, 122
client
  e-mail, 89
COM
  protocols, 39
Command Line Interface, 122
configuration, 23
conformity, 137
connecting M!DGE, 20
connectors
  Antenna SMA, 12
  ETH RJ45, 13
  screw terminal, 13
  USB, 13

D
declaration of conformity, 137
demo case, 19
digital I/O, 53
dimensions, 12
dynamic DNS, 88

E
e-mail, 89
ethernet, 28
event manager, 90

F
F bracket, 18
factory reset, 109
features, 17
  key features, 7
file configuration, 107
firewall, 61

G
glossary, 141
grounding, 22

H
home, 23

I
implementation notes, 11
indication LEDs, 16
installation, 22
interfaces, 24
IPsec, 70

K
keys, 115

L
LAN cable, 20
LED, 16
legal notice, 119
licensing, 119
logout, 121

M
menu
  firewall, 61
  home, 23
  interfaces, 24
  logout, 121
  routing, 54
  services, 78
  system, 101
  troubleshooting, 109
  VPN, 67
mobile, 32
models, 18
mounting, 22

O
offerings, 18

P
power supply, 22
  connect, 20
product
  Conformity, 137
protocols COM, 39
protocolserver, 39

R

redundancy, 99
reset, 109
ROHS, 138
router, 7
routing, 54

S

safety instructions, 137
serial port, 37
server
  DHCP, 86
  dial-in, 77
  DNS proxy, 87
  PPTP, 75
  SSH/Telnet, 95
  web, 98
services, 78
SIM, 32
SIM card, 20
SMS, 92
SNMP agent, 96
software update, 104
specification, 17
standards, 8
start, 6
system, 101
  restart, 102
  settings, 101

T

technical specification, 17
time&region, 102
troubleshooting, 109, 135

U

update, 104
USB, 35

V

VPN, 67

W

WAN, 24
web configuration, 23
WEEE, 138

Appendix B. Revision History

Revision 1.1 2012-10-09
1st XML version

Revision 1.2 2012-12-07
Updated chapter 7 for FW version 3.6.40.x

Revision 1.3 2012-12-12
Updated chapter 8 – Command Line Interface

Revision 1.4 2013-10-09
Added section the section called “Protocol Server”

Revision 1.5 2014-09-04
Added information about Country of Origin
Complete manual revision for FW version 3.6.41.x

Revision 1.6 2014-04-09
Complete manual revision for FW version 3.7.40.x

Revision 1.7 2015-01-10
Added section Section 7.7.8, “Legal Notice”,

Revision 1.8 2015-11-03
Complete manual revision for FW version 3.8.40.x